A FRAMEWORK FOR SECURITY PREVENTION FROM VARIOUS ATTACKS ESPECIALLY IN ONLINE E-TRANSACTION

A Dissertation

Submitted

In Partial Fulfilment of the Requirements for

The Degree of

MASTER OF TECHNOLOGY

In

Computer Science & Engineering

Submitted by:

Mohammad Salman Husain

Under the Supervision of:

Dr. Mohammad Haroon

Department of Computer Science & Engineering

Faculty of Engineering

INTEGRAL UNIVERSITY, LUCKNOW, INDIA

August, 2020

DECLARATION

I hereby declare that the Dissertation titled "**A Framework for Security Prevention from Various Attacks Especially in Online e-transactions**" is an authentic record of the research work carried out by me under the supervision of **Dr. Mohammad Haroon**, Department of Computer Science & Engineering at Integral University Lucknow. No part of this Dissertation has been presented elsewhere for any other degree or diploma earlier.

I declare that I have faithfully acknowledged and referred to the work of other researchers wherever their published works has been cited in the Dissertation. I further certify that I have not willfully taken other's work para text data results table figures etc. reported in the journals, books, magazines, reports, dissertation, etc. or available at websites without their permission and have not included in this M.Tech. Dissertation citing as my own work.

Date:
Place:

Signature

Mohammad Salman Husain
Enrollment no. 1700103567

CERTIFICATE

This is to certify that Mohammad Salman Husain (Enrollment no. 1700103567) has carried out the research work presented in the dissertation titled "**A Framework for Security Prevention from Various Attacks Especially in Online e-transactions**" submitted for partial fulfilment for the award of **Master of Technology in Computer Science & Engineering** from **Integral University, Lucknow** under my supervision.

It is also certified that:

(i) This dissertation embodies the original work of the candidate and has not been earlier submitted elsewhere for the award of any degree/diploma/certificate.

(ii) The candidate has worked under my supervision for the prescribed period.

(iii) The dissertation fulfills the requirements of the norms and standards prescribed by the University Grant Commission and Integral University, Lucknow, India.

(iv) No published work (figure, data, table etc) has been reproduced in the dissertation without express permission of the copyright owner(s).

Therefore, I deem this work fit and recommend for the submission for the award of the aforesaid degree.

Signature of Supervisor

Full Name: Dr. Mohammad Haroon
Designation: Associate Professor
Department: Computer Science & Engineering
Address: Integral University, Lucknow
Date:
Place: Lucknow

Signature of H.O.D.

Dr. Mohammadi Akheela Khanum
Head of Department
Computer Science & Engineering
Integral University, Lucknow

COPYRIGHT TRANSFER CERTIFICATE

Title of the Dissertation: **A Framework for Security Prevention from Various Attacks Especially in Online e-transactions**

Candidate Name: **Mohammad Salman Husain**

The undersigned hereby assigns to Integral University all rights under copyright that may exist in and for the above dissertation authored by the undersigned and submitted to the University for the Award of M.Tech. degree.

The candidate may reproduce or authorize others to reproduce material extracted verbatim from the dissertation or derivate of the dissertation for personal and/or publication purpose(s) provided that the source and the university's copyright notices are indicated.

MOHAMMAD SALMAN HUSAIN

ACKNOWLEDGEMENT

I am highly grateful to the Head of Department of Computer Science and Engineering for giving me proper guidance and advice and facility for the successful completion of my dissertation.

It gives me a great pleasure to express my deep sense of gratitude and indebtedness to supervisor **Dr. Mohammad Haroon Associate Professor, Department of Computer Science & Engineering,** for his valuable support and encouraging mentality throughout the project. I am highly obliged to him for providing me this opportunity to carry out the ideas and work during my project period and helping me to gain the successful completion of my project.

I am also highly obliged to **Dr. Mohammadi Akheela Khannum (Associate Professor and Head of the Department, Department of Computer Science & Engineering)** and PG Program Coordinator **Dr. Faiyaz Ahmad, Assistant Professor, Department of Computer Science & Engineering,** for providing me all the facilities in all activities and for his support and valuable encouragement throughout my project.

My special thanks are going to all of the faculties for encouraging me constantly to work hard in this project. I pay my respect and love to my Parents and all other family members and friends for their help and encouragement throughout this course of my project work.

Date:
Place: Lucknow

Mohammad Salman Husain
Enrollment No. 1700103567

TABLE OF CONTENTS

LIST OF TABLE

LIST OF FIGURES

LIST OF SYMBOLS & ABBREVATIONS

PAKE	Password Authentication Key Exchange
KGC	Key Generation Center
TPA	Third Party Auditor
PPDM	Privacy Preserving Data Mining
GKE	Group Key Establishment
TTP	Trusted Third Party
TAN	Transaction Authorization Number
MTA	Mail Delivery Agent
MUA	Mail User Agent
MD-5	Message Digest -5
CHAP	Challenge Handshake Authentication Protocol
ECC	Elliptic Curve Cryptography
IDA	Identity Disclosure Attack

ABSTRACT

Security in various E-commerce Applications includes an efficient framework in Information Security especially in Computer Security, Data Security and other online transactions in E-commerce applications. Security in E-Commerce application plays an important role for the secure and scalable transaction which includes various dimensions such as security-integrity, Confidentiality, Non-repudiation, Privacy etc. Hence for the Security of Online Transactions in E-Commerce based application various Security algorithms are implemented. Although these Security algorithms are efficient and provides Security from various attacks but Data Storage during the transactions and Computational time of the algorithms is also important.

The existing architecture proposed for the security of online e-transactions in web applications provides security from different attacks and is efficient in terms of computational parameters, but there are certain issues which need to be overcome such as: Security Prevention from different attacks during Online Transactions in Web Mining especially in E-commerce Applications, Increase use of Computational Cost at the Client and Server Side.

The Proposed framework provides Security prevention from various attacks especially in IoT. The methodology implemented here works on the basis of authenticating the validity of the User by allocating a challenge value and hope that our proposed framework will be more effective and efficient.

E-commerce in today's world is playing an inevitable role. As much as technology makes things easier for us, it makes ourselves open to online attacks. Say for a banking transaction, all we have to do is login to our account and do the transaction. Currently, financial sites use static passwords, which are easier for customers to use. These can also potentially put the user's account into risk. Given enough time and number of attempts, an attacker can easily access login. Static passwords can be vulnerable to attacks such as shoulder-surfing, dictionary attacks and so on. By constantly altering the password, as is done with a one-time password, this risk can be greatly reduced.

We propose a system with a different perspective of password security targeting online financial websites. E-commerce applications use OTP to provide security by changing the password every time, so OTP is preferred. For personal recognition biometric technique such as fingerprint or palm-vein scan, etc., can be used. Unlike other biometrics, fingerprint is unique. Noisy password is a strong alternative for static password. Hence, we are trying to incorporate a combination of all the three to provide a secure method to perform E-transaction in E-commerce applications.

CHAPTER 1

INTRODUCTION

1.1 BACKGROUND

What is online payment?

Online payment, also known as electronic payment, it refers to the money which exchanged electronically. Broadly speaking, online payment refers to the transaction exchanged the funds on internet, typically involves computer network, internet and digital stored value system. It makes e-payment may at any time, via the internet directly to the transfer, settlement, and forms of e-commerce environment.

How online payment basic process?

Online payment may seem to be very easy and fast, but it consist of the confidential and security for the card info. In order to make sure that the process is work correctly, the merchant must connect to the network with the Issuing bank, processor, and others financial institution, so that the information that provided by the customer can be routed reliable and secure. As highly sensitive payment information, trust and confidence is an essential element of any payment transactions. This means that payment processing services should be provided by a wealth of experience in payment processing and security.

What is electronic commerce?

Electronic commerce refers to the goods and services which exchange over the internet, commonly known as e-commerce. All major retail organization also have an online presence, however, e-commerce also apply between business to business (B2B) transactions. It can open to all interested parties, or even limited participants. For example

like Amazon.com, the selling and buying transaction is completed electronically and interactively in real-time. Besides that, e-commerce system also associated with the service industry, such as online banking, transfer funds, or even pay the credit card bill.

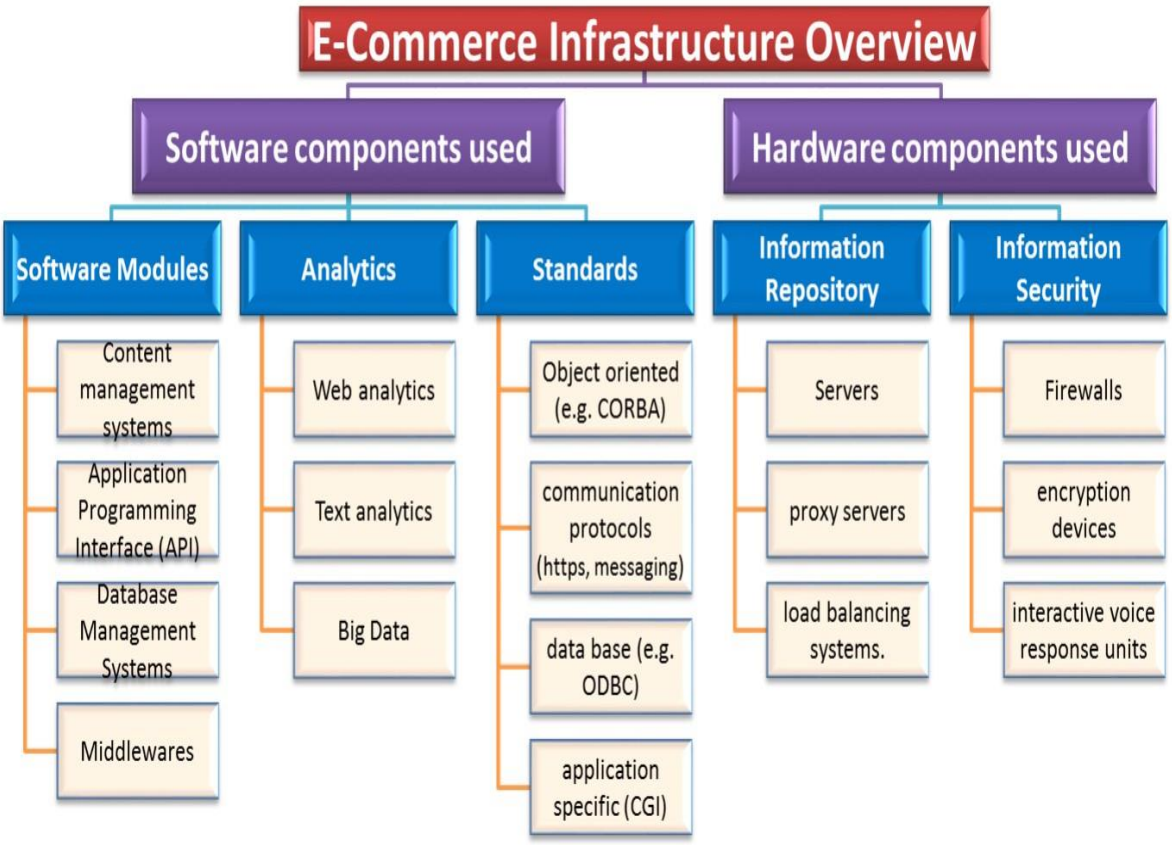


Figure 1.1: E-Commerce Infrastructure Overview

1.2 PROBLEM STATEMENT

Security in various E-commerce Applications includes an efficient framework in Information Security especially in Computer security and Data Security and other Online transactions in E-commerce applications. Security in E-Commerce application plays an important role for the secure and scalable transaction which includes various dimensions

such as security-integrity, Confidentiality, Non-repudiation, Privacy etc. Hence for the Security of Online Transactions in E-Commerce based application various Security algorithms are implemented. Although these Security algorithms are efficient and provides Security from various attacks but Data Storage during the transactions and Computational time of the algorithms is also important.

- **Security of e-commerce**

Along with the e-commerce continue to broaden, protection of individual treatment over the internet, and make your customers feel secure is the primary factors and necessary. In order to perform a secure and good service, internet security plays an important role to be enhancing in this situation. The objective is to establish rules and measure to use against attacks over the Internet. Internet information exchange on behalf of the invasion led to unsafe or high risk of fraud.

For any expert in internet security will tell, e-commerce is actually much more secure than real world commerce. For example when you leave your credit card receipt in the shop, or accidentally give your credit card number to someone else, you are actually accepting the risk that the order which not order from you will appear on the next month's credit card bill. However, when you enter a credit card number of e-commerce site, you are sent through a secure connection to a server access only to authorized personnel and protected against even the most determined intruders.

Although some of the people believe that transactions over the internet are in fact safer than offline transactions, there are still a number of people believe that offline transactions are always better than online payment. For example like protecting the credit card detail,

company need to prevent the card info from customer or the privacy of the customer found by a third party. Typically, this involves the company network security and how the company provides a strong and secure system on the internet.

1.3 Common Online Payment System

Online payment system is to help the consumer more convenience and it is the key issue to ensure that the consumer are fast and secure. There are several types of common online payment systems:

- **E-cash internet payment system**

E-cash, also known as electronic cash or electronic money, it is a form of data which exchanged electronically through the network computer or internet, these is electronic cash currency. It can be converted to cash value of the family of cryptographic sequences, and then use these sequences to show the value of all sizes. There are few characteristic are as follows: an agreement between the enterprises and banks and authorization, can be transfer, can be kept, used to exchanged value within another system.

As e-cash is what we can imagine as “cash” China’s purchase of small general merchandise payment habits features, it is likely to become an important means of online payment in China, but China has not officially started. There are many foreign companies to provide electronic cash market. If unconditionally anonymous electronic money digital cash net cash market can provide an anonymous e-money market.

- **E-purse Internet Payment System**

E-purse, also known as electronic purse, it is a type of smart card which embedded with the microchip. To use e-purse shopping, the first is the user must transfer certain amount of personal bank account, then in the corresponding of website to download electronic wallet service system free software and install an electronic wallet, to apply online and access the cardholder “electronic safety certificate. When users want to purchase something through the internet, just need to click on the “electronic wallet” icon, and follow the corresponding information that the user need to provided, such as password and user name to complete the transaction on the internet.

E-purse would be more convenient and flexible compared with checks or debit card for a smaller transaction, it always used in conjunction with the bank card to help the user complete all the small transaction process. E-purse is independent of the function of bank accounts, so it will be able to record the user as required payments are made in a checkbook greater privacy and freedom. In addition, e-purse even can provide budgeting because the user only can spend what the total amount that the card had.

- **Electronic check (E-check) Internet Payment System**

Electronic check, also known as e-check, is a form of payment which transfers through the internet. It performs the same function as the paper check of using digital transmission to transfer money from one account to one account. Besides that, e-check provide better security features than the paper check because it is an electronic format and may proceeded in fewer steps to complete the transaction. Most common features provided by electronic

checks include authentication, public key cryptography, digital signatures or personal identification numbers instead of signature and so on. There's a simple electronic check process shown below:

1. Send Check
   Payee
   Payer
2. Inspect Check
3. Bill
4. Notice
5. Approve funds and transfer
   Payee Bank
   Accounting Server
   Electronic Check-Cashing Process

E-check is an exclusive network system, the international financial institutions, with their equipment, software and hardware, an accurate and complete set if user identification, the standard messaging, data validation and other standardized data transmission agreement to make sure that the transaction are safety and security.

- **Digital Wallet Payment System**

A digital wallet, also known as e-wallet, it is a software system that store inside the user's computer to hold the digital cash, and a digital certificate with a digital signature. E-wallet allows users to make payment or transaction over the internet fast and safety. The function of the e-wallet is much more like a physical wallet, used to store the digital cash. After the e-cash service released, the e-wallet has evolved into a service to provide online shopping

information and holds credit card data and passwords for logging into the website with a convenient way.

An e-wallet have both software and information component. The software provides the safety and security with the encryption for the actual transaction. Typically, e-wallet is store on client side, so it is easier to self-maintenance and fully compatible with most of the online payment system. In addition, the system will automatically key in the user information in the online form, it is easier for the user and reduce the time to enter all the information again and again. While for the server side, it is refers to an organization and your side to create and maintain on it server. Because of the security and the efficiency and effectiveness of the utility that provided by the server-side to the users, it become more and more popular and famous for the user with the entire process.

- **PayPal System Listen**

PayPal is an e-commerce business by allowing the user to make transaction or money transfers through the Internet. PayPal also known as electronic alternative, such as checks and money are orders with the traditional paper method. It doesn't charge any fees to make any transaction or join the PayPal service, but they will be a fees change for those who want to receive the money from other people.

PayPal account from a bank account can be funded by electronic debit or credit card. To receive the transaction from other people, the recipient from PayPal can either request from the PayPal service, established their own PayPal account, or request from their bank account. PayPal service is much like a intermediaries or a third party who involve between the clients and the recipient that facilitates in e-commerce.

PayPal involve in several payments processing such as, online auction, online vendors, and others commercial users. It will cost some fees from the recipient for receiving money; fee included the percentage of the amount plus another additional amount. The fees is charged depend on the currency used, the option that choose by the user, the country of the sender and recipient (how far between both sender and recipient), the total amount sent by the sender and the type of account that the recipient receive it. In addition, shopping on eBay and then made the transaction by a credit card through PayPal may incur a "foreign transaction fee" if the seller is located in another country, as credit card issuers are automatically informed of the seller's country of origin.

Critical Evaluation

According to Singh Sumanjeet1 (2009, p.24), Electronic cheque system has many advantages: (1) they do not require consumers to reveal account information to other individuals when setting an auction (2) they do not require consumers to continually send sensitive financial information over the web (3) they are less expensive than credit cards and (4) they are much faster than paper based traditional cheque. But, this system of payment also has several disadvantages. The disadvantage of electronic cheque system includes their relatively high fixed costs, their limited use only in virtual world and the fact that they can protect the users' anonymity. Therefore, it is not very suitable for the retail transactions by consumers, although useful for the government and B2B operations because the latter transactions do not require anonymity, and the amount of transactions is generally large enough to cover fixed processing cost.

In my opinion, i strongly agree with the statement that the author mentioned about. Electronic cheque system provides several advantages than a paper based cheque such as

faster speed transaction, provide a certain level of security like encryption or decryption, and so on. But there are still limits of disadvantages for electronic cheque system, like high fixed costs or development start-up costs. Besides that, electronic cheque system can be used in virtual world instead of the real world payment method. And the most important point is the security issue, because the less of face to face communication, we can't even know the actual user as well. The possibilities that someone is try to pretend as the actual user to make transaction with us and caused identity threat

- Strength and Weakness
- Advantages of Online Payment

Online payment, what we called as online payment, is an indispensable business. This is extremely important to accept electronic payment of telecommunications service industry, because it started to use this rapidly growing economy is fully utilized.

Use of credit cards by phone or Internet is a familiar and convenient for consumers in the form of payment. It provides for immediate purchase to reduce the pain of payment delay coupling. Customers often feel more comfortable with a credit card, because they know they have the proof to the product or service if they not satisfy on it.

1.4 There are several advantages of online payment (e-payment):

- **Convenient and 24 hour's real time transaction**

Through the use of online payment system, consumer can access the web to make any transaction such as online banking, online billing or even car loan at any time (24 hours) or anywhere, as long as access to the internet. For example like consumer can check the bank details through their mobile phone no matter at where and anytime along with the network

connection. In addition, consumer able to check or view the history of the previous transaction that they made or get the accurate real time information through online payment system. It may save up a lot of the paperwork as well.

- **Reduce cost and save time**

With the help of online payment system, we only need to stay at home with just a click in front of the computer which connected to the network, and transaction will be done easily. Instead of go to the physical bank to make the transaction by writing the form and waiting in front of the counter. It may save up a lot of cost like transportation fees, paper workflow fees and so on.

Besides that, through online payment, the processing speed is definitely fast and rapid by following the simple instructions and entering the parameters that the system required. And user may not need to transport from one location to another, it may save up a lot of time. Compared with the real world physical offline banking system, it may spend a lot of time especially on peak season or peak hour.

- **Flexible of using e-payment**

Along with the continuous improvement of e-commerce, many organizations or firms not only focusing their business on offline operation, but managing their business workflow on internet. Nevertheless, e-payment, as what we called as online payment, had become an indispensable item for the entire progress of e-business. Nowadays, there are more and more online payment service provided which linked with the organization. It is more

flexible to the consumer, they can choose which type of service that they want, for example like PayPal, e-cash or which bank they prefer such as maybank2u and so on.

Besides that, majority of the online payment service are operation 24 hours, consumer can make the transaction anytime they like. In addition, they can reduce they pain of transport from one location to another and waiting in-front of the counter in the bank. Online payment service allow consumer to make any transaction on anytime or everywhere by accessing to the network. It is the flexibility of e-payment.

- **Benefit between consumer and organization**

With the help of online payment, consumer and organization are benefiting in other ways like the consumer and organization are able to negotiate arrangements for the true value, and strengthen the relationship of their business.

Besides that, consumer can skip many steps or documentation for the transaction. It may easier for them to control over the timing of payment steps, and minimize the operation of the idle account balance. Consumer can eliminate the delay for the processing of transaction. For organization, they can reduce the cost of processing the paper cheque. Yet when the organizations process the paper cheque that paid from consumers, they need to spend some cost to process the paper cheque.

With the help of online payment, the organization may have the advantages as well by encouraging the consumer to pay electronically instead of pay by a paper cheque. In addition, they can receive the payment immediately without any delay, because the receipt is available immediately after consumer had made the payment.

- **Others common benefits**

Below are some of the common benefits for online payment method.

Personal security

We do not need to hold so much money along with us on our premises, or even on the outside, and lead to more safety and security.

Used internationally

Online payment is a common method that can be used internationally, it is important for the tourist-sector businesses or those organization who running their business or selling their goods overseas.

Reaching a wider customer base

Some of the organizations accept the online payment method like phone delivery or mail ordering for online customers; it is easier for those customers who are lack of transportation or not able to reach your premises.

Increase the sale opportunities

For some customer willing to buy the goods from the offline business shop, the may having the problem that insufficient fund, they have to leaves to get cash, it may cause them not return to the shop again.

With the help of online payment from ecommerce sector, customer can buy the goods from internet as long as the computer or devices are connected to the internet. This may lead to sale increasing.

1.5 Disadvantages of Online Payment

The transaction over the internet or the transfer of fund on internet through the electronic media is known as electronic payment, as what we called as online payment. Nowadays, online payment is a daily activity for most of the business organization. It is very common and convenient for the online transaction for those organizations focus their business over web to interact with their consumers or business partners. In fact, there are still weaknesses of the online payment that we cannot ignore it. One of the ways is to be aware the raised awareness of privacy and security issues from the electronic online payment system. Consumers have to bear the risk such as fraud or identity threat that involved in the online transaction.

There are several disadvantages of online payment (e-payment):

- **Privacy security concerns.**

In the e-commerce world, most of the online banking systems, also known as online transaction site, require the user to register as their own member with some simple input or instruction before giving the authorization for them to make the transaction. While the registration process, user need to provide the username and password, all these information implies the need of privacy protection and security. In addition, user need to maintain their account, it may be a trouble for the user.

For those organizations' site that hosting the user account, they should follow the strict of security and privacy policies. It is very important for those organizations to protect the privacy of the user details and prevent the information being hacked by the hacker. If the

username or password is susceptible to being hacked, it maybe will cause the user a serious financial loss problem from the end. All these are a potential rick of the privacy or the personal detail being hacked while using the online payment system.

- **Identity theft**

Another disadvantage of using online payment is identity theft. Using the right security measure can prevent your important information being exposed by the third party. Besides that, using virus protection or firewall may very useful to protect your computer. It might a risk that you make any transaction through internet from your computer.

Another example like if you losing your smart card, unfortunately the card is fall in unsafe of person's hand. There is a very serious or dangerous expenditure of your entire account balance. Though you will inform the authorities on card's loss, when the time between you losing your card and informing to the authorities, the third party (unsafe person) may transfer all your money out through your card details via internet.

- **Dependency of online payment system**

Along with the information technology, many organizations or firms are running their business over the internet and provide several utilities as long as online transaction. In fact, this method is indirectly effect consumers become more and more dependent on online transaction, because it speed and rapid transaction, availability 24 hours as long as connected to the internet at home or even a mobile devices.

However, there still can be disadvantages for over dependent of online transaction. For example like if the email does not send to the right destination or not working well, the

sender may not know the sending error or does the email has reach the destination or not. Or like for those consumers may want to pay the bill or loan over the internet instead of the traditional ways. There might be a possibility that the online payment system down or not function well from the server side, and worst there was a way for the consumer to meet the dead line.

- **Loss human touch**

In the physical bank, some of the customer may like to talk and communicate with the bank tellers, interacting with the bank manager or even the bank clients. But in the online virtual world, online banking system had taken off of these “human interactions”; all these are done by a system program, impersonal hand-off process.

Due to the lack of the “human interaction” for online payment system, some of the customer my not know about the knowledge of online payment system. These required a basic computer skill and the knowledge about internet before using the online payment system. In addition, for some of the small online banking system, they may not provide any instruction or any guideline to lead the user in the correct way. It will cause the users entering the wrong information or incorrect bank details through the online payment system.

- **High cost development for internet payment gateway**

The major disadvantage for online payment method is the high cost for internet payment gateway. For those organizations or firms are running their business over the internet, the have to create an internet payment gateway or a system in-house is definitely high

development cost. For those non IT companies, it is hard and difficult for them to create a system for their own. Because it wasn't their core business, and they had to use the resource from inside the company with a little or even zero of IT knowledge to build it up. Therefore, the company have to outsource from outside to help them develop a new online payment gateway for them.

- **Others Limitation**

Others common limitation of the online payment method:

May be difficult to inspect from a remote location

Limited of countries cultural and legal obstacles

The rapid changing of technologies

Hard to retaining the employee

Government regulators

Difficult to integrate the software of transaction process and the current existing database.

Critical Evaluation

Based on Olga Lu et.al (2009, p.15-16) The main benefit from the bank customers' point of view is significant saving of time by the automation of banking services processing and introduction of an easy maintenance tools for managing customer's money. Private customers seek slightly different kind of benefits from e-banking. In the study on online banking drivers Aladwani (2001) has found, that providing faster, easier and more reliable services to customers were amongst the top drivers of e-banking development.

In my opinion, I definitely agree with the above statement that stated by author (Olga Lu et. al). Online payment may help to reduce costs and convenience; user may stay at home

to performed transaction at any time as long as connected with the network. It is fast and provides funds management, which allow user to download the history of the transaction that that had made.

1.6 Ecommerce Security Elements

In the use of ecommerce, there are several factors that need to involved are: the confidentiality and privacy of the transaction need to be care between the sender and the recipient. The transaction or trading from ecommerce is directly represents to the individual, organization, or business competitor secrets. Therefore, to prevent any confidential data lost from ecommerce application, we have to make sure that the users are legitimate to access the system, and the authentication to filter which date should be show or which should not be show to the particular user.

- **The Integrity of the information**

Due to the accident or fraud of data entry, the information of the data may result in different way. In addition, the wrong of data or information will result the duplication of transmission in different sector of the process. Therefore, the trade sector will affect the integrity of the information from the parties that involved in the transaction and the entire of the business workflow.

- **The validity of the information**

In e-commerce world, the validity of information to individuals, organizations or even the countries are directly affected to the economic interests and reputation. Besides that, the

validity of the number of time and the transaction price are very important. It is to make sure that the recipient received the data from the primary side. While for the primary side also have to make sure that the data are sent to that particular person.

- **The Non-repudiation of the information**

Non-repudiation is refers to something like document or contract that cannot simply denied by the origin party. Typically, non-repudiation is to ensure that the contract or one party cannot deny that they communicate to sign the document or the authenticity of a message. For example like legal documents usually need a witness person to sign it, it is to ensure that the person cannot deny the document.

- **The Authenticity of the transaction status**

Online transaction are geographical distant, we couldn't know each other or even an organization. Organization, businessmen, client or even consumer on internet may need to consider whether the transactions between both parties are trusted. To make the transaction success, mutual understanding and trusted with each other is very important.

However, there are too many hacker or scammer in the virtual world, is hard to 100% fully trusted on the online transaction or even the in the virtual organizations.

- **The reliability of the system**

In e-environment, the most important point for the reliability of the system is to protect the confidentiality with a powerful security system. In addition, it is to prevent hacker hack into the system and steal the sensitive information from the system. Computer errors such

as system failure, software down, virus detected, network connection down or natural disasters may result from potential threat.

Therefore, prevention of the system in a good way is to ensure that the systems are security and reliability. It will affect the business workflow in the future if the reliability of the system is not fully secure.

Critical Evaluation

According to the Yang Jing (2009, p.48), using the network for the transaction, the sender and recipient need to ensure the confidentiality of information exchanged. E-commerce as a means of trading, its message directly represents individuals, corporations or commercial secrets; and the e-commerce system is based on a more open network environment promote the application of ecommerce to maintain commercial confidentiality is an important guarantee. Therefore, in order to prevent a large number of transmissions was illegal to steal information to ensure that only legitimate users will be able to see the data. Information can prevent stolen.

In my opinion, I absolutely agree with the statement that the author status above. To prevent the information lost, we have to protect it before happen. The integrity of information, the validity of information, the non-repudiation of information, The Authenticity of the Transaction Status, and The Reliability of the System, all these are the important elements which listed by the Author (Yang Jing) to prevent information lost. In fact, I believe that there are still a number of elements for information prevention which I never mentioned on top.

1.7 Two Servers Password Authentication

Two server PAKE (Password Authentication Key Exchange) use symmetric solution to authenticate client in client server authentication system. This system have advantage that encrypted password get store in two servers instead of single server to minimize disadvantage of single server system. Both the servers communicate and exchange messages to authenticate client. OPT (One Time Password) is also a secure solution which uses random function to generate password and this password get discard after one use. In this paper, two server PAKE and OTP protocol is combine to overcome drawback of previous systems and provide more security. First two server PAKE will run to store the encrypted password in two server and then to authenticate the client OTP protocol send OTP on the client's mobile. Only using this OTP the client will get the authenticated.

Passwords are one of the important factor of security which is used in day to day life for logging process into the computer system, mobile phones etc. Also along with the password importance, security of it is one of big issue. Authentication systems based on user id and password are very efficient and are low cost systems. Previously there was single server system where all the passwords were stored which was a vulnerable system .If that server gets compromised then all passwords were disclosed. Passwords can be easily cracked because of single point failure. Password authentication key exchange is where client and server communicate with each other using the cryptographic key. The two solutions for PAKE are symmetric and asymmetric solutions. Symmetric is where both the servers work together to authenticate the client. In Asymmetric solution one server takes the help of another server to authenticate the client. In symmetric solution

both the servers and client establishes a secret key session. Asymmetric solution works in series and only client and the main server needs to establish secret key. Symmetric protocol works in parallel which makes it reliable than asymmetric system. To address the issue of single server system we are going use the concept of multiple servers.

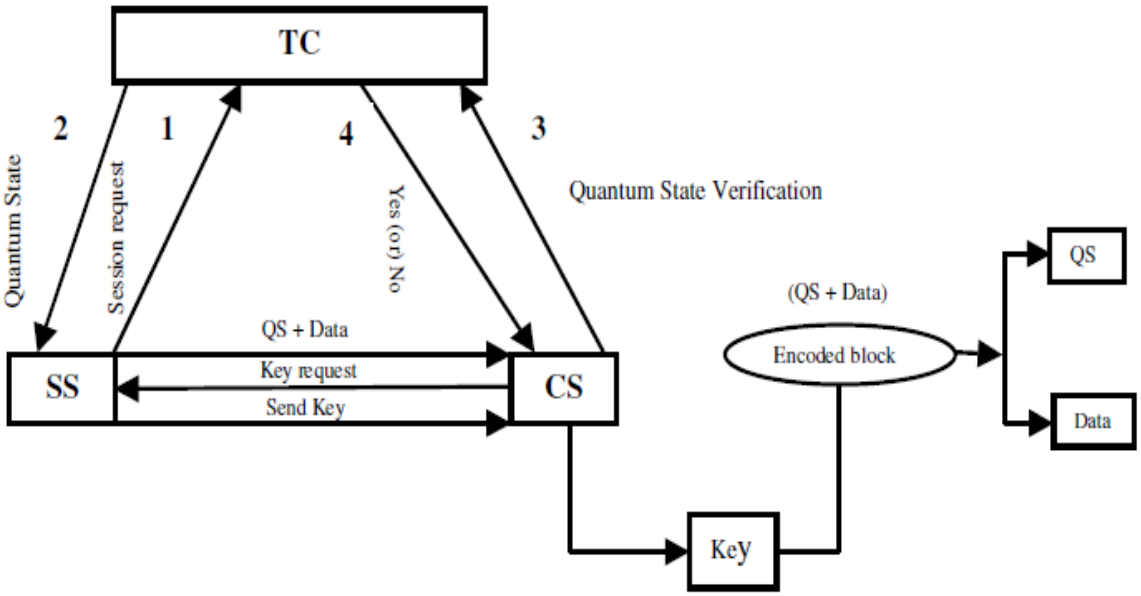


Figure 1.2: Process Flow Diagram for Quantum Based Two Server Passwords Authentication (SS-service server, CS-control server)

1.8 Strategic of E-commerce Security

As e-commerce security cause by many factors such as fraud, identity theft, or confidential data being steal by the hacker, all these are the problem that we might face it when in the online virtual world. So, a strategic planning for ecommerce is very important, all the strategic that came out should be line with the overall of the ecommerce business management. It must provide a very powerful protection for all the ecommerce

confidential data and allow them to recover as fast as possible if any incident happen. To prevent the security problem happen, a set of variety measurement must be included.

1.8.1 Security Strategy

In order to ensure secure communications between both parties on internet, we must take the necessary measures to prevent them. For communication link purpose, we can use firewall or Virtual Private Network (VPN) to make the communication more safety and secure. And consumer must be very careful on some of the untrusted Proxy server. It is act like an intermediary for seeking the information, resource, or link that requested by the client. If the consumer are using the untrusted proxy server, all the data that the client provided may not be encrypted and sent to the proxy server, and proxy server may record down everything sent from the client, including the login and password.

For identification and authentication purpose, encrypted or hash function may be very useful in this situation. In ecommerce, login is a very common and the first step for the consumer before they move on the transaction step. To login to the system, the system needs to identify the user name and password before provide the authentication to the user. With the help of encryption, user password have more secure which showing the password in "*" symbol.

In order to provide security to the customer, existing banking system uses various level of security mechanisms. Even though tough encryption standards are provided against network attacks, it is prone to be broken. Intruders are smart enough to retrieve the passwords of the customers through online transaction. As per the world payments report, in current technology people prefer to use cashless payments rather than the cheques or

cash payments. As we all know that these kinds of e-transactions provide huge number of benefits to the customers for example, by making the transactions easier, faster and instant payments. As per the survey an Indian uses online transaction system once in a week for payment. This online transaction might be through credit/debit cards, e-wallets, UPI's, food cards, travel cards and some authorized e-payment systems. Many security implementation methods like hardware level security, antivirus, anti- malware and antispyware programs, strong passwords, single time bound OTP system, virtual private network, secured site uses SSL certificate are used in practice. However, in spite of all these security mechanisms intruders go for brute force attempts to decrypt the PIN numbers and passwords etc. So, single level encryption standard is not sufficient to provide high level security for online transaction system. At present we need to have a multilevel encryption standard wherein even if anyone encryption standard is broken, the online transaction requested by the customer will be completed with the other encryption standard. Our paper focuses on multilevel security with Blowfish and AES algorithm along with dual OTP scheme which may lead to stronger level of protection against threat encountered in online transactions.

E-Commerce refers to the activity of buying and selling things over the internet. Simply, it refers to the commercial transactions which are conducted online. E-commerce can be drawn on many technologies such as mobile commerce, Internet marketing, online transaction processing, electronic funds transfer, supply chain management, electronic data interchange (EDI), inventory management systems, and automated data collection systems. E-commerce threat is occurring by using the internet for unfair means with the intention of stealing, fraud and security breach. There are various types of e-commerce threats. Some

are accidental, some are purposeful, and some of them are due to human error. The most common security threats are an electronic payments system, e-cash, data misuse, credit/debit card frauds, etc.

1.9 Electronic payments system:

With the rapid development of the computer, mobile, and network technology, e-commerce has become a routine part of human life. In e-commerce, the customer can order products at home and save time for doing other things. There is no need of visiting a store or a shop. The customer can select different stores on the Internet in a very short time and compare the products with different characteristics such as price, colour, and quality.

The electronic payment systems have a very important role in e-commerce. E-commerce organizations use electronic payment systems that refer to paperless monetary transactions. It revolutionized the business processing by reducing paperwork, transaction costs, and labour cost. E-commerce processing is user-friendly and less time consuming than manual processing. Electronic commerce helps a business organization expand its market reach expansion. There is a certain risk with the electronic payments system.

1.9.1 Some of them are:

- **The Risk of Fraud**

An electronic payment system has a huge risk of fraud. The computing devices use an identity of the person for authorizing a payment such as passwords and security questions. These authentications are not full proof in determining the identity of a person. If the password and the answers to the security questions are matched, the system doesn't care

who is on the other side. If someone has access to our password or the answers to our security question, he will gain access to our money and can steal it from us.

- **The Risk of Tax Evasion**

The Internal Revenue Service law requires that every business declare their financial transactions and provide paper records so that tax compliance can be verified. The problem with electronic systems is that they don't provide cleanly into this paradigm. It makes the process of tax collection very frustrating for the Internal Revenue Service. It is at the business's choice to disclose payments received or made via electronic payment systems. The IRS has no way to know that it is telling the truth or not that makes it easy to evade taxation.

- **The Risk of Payment Conflicts**

In electronic payment systems, the payments are handled by an automated electronic system, not by humans. The system is prone to errors when it handles large amounts of payments on a frequent basis with more than one recipients involved. It is essential to continually check our pay slip after every pay period ends in order to ensure everything makes sense. If it is a failure to do this, may result in conflicts of payment caused by technical glitches and anomalies.

Vishing/Phishing

Phishing is an activity in which an intruder obtained the sensitive information of a user such as password, usernames, and credit card details, often for malicious reasons, etc.

Vishing is an activity in which an intruder obtained the sensitive information of a user via sending SMS on mobiles. These SMS and Call appears to be from a reliable source, but in real they are fake. The main objective of vishing and phishing is to get the customer's PIN, account details, and passwords.

Online Transaction

Online transaction can be made by the customer to do shopping and pay their bills over the internet. It is as easy as for the customer, also easy for the customer to hack into our system and steal our sensitive information. Some important ways to steal our confidential information during an online transaction are-

- By downloading software which scans our keystroke and steals our password and card details.
- By redirecting a customer to a fake website which looks like original and steals our sensitive information.
- By using public Wi-Fi

POS Theft

It is commonly done at merchant stores at the time of POS transaction. In this, the salesperson takes the customer card for processing payment and illegally copies the card details for later use. Ecommerce security is the guidelines that ensure safe transaction through the internet. It consists of protocols that safeguard people who engage in online selling and buying of goods and services.

You need to gain your customers' trust by putting in place ecommerce security basics. Such basics include:

- Privacy

- Integrity
- Authentication
- Non-repudiation

- **Privacy**

Privacy includes preventing any activity that will lead to the sharing of customers' data with unauthorized third parties. Apart from the online seller that a customer has chosen, no one else should access their personal information and account details.

A breach of confidentiality occurs when sellers let others have access to such information. An online business should put in place at least a necessary minimum of anti-virus, firewall, encryption, and other data protection. It will go a long way in protecting credit card and bank details of clients. Information should not be accessible to an unauthorized person. It should not be intercepted during the transmission.

- **Integrity**

Integrity is another crucial concept of ecommerce Security. It means ensuring that any information that customers have shared online remains unaltered. The principle states that the online business is utilizing the customers' information as given, without changing anything. Altering any part of the data causes the buyer to lose confidence in the security and integrity of the online enterprise. Information should not be altered during its transmission over the network.

- **Authentication**

The principle of authentication in ecommerce security requires that both the seller and the buyer should be real. They should be who they say they are. The business should prove that it is real, deals with genuine items or services, and delivers what it promises. The clients should also give their proof of identity to make the seller feel secure about the online transactions. It is possible to ensure authentication and identification. If you are unable to do so, hiring an expert will help a lot. Among the standard solutions include client logins information and credit card PINs. There should be a mechanism to authenticate a user before giving him/her an access to the required information.

- **Non-repudiation**

Repudiation means denial. Therefore, Non-repudiation is a legal principle that instructs players not to deny their actions in a transaction. The business and the buyer should follow through on the transaction part that they initiated. Ecommerce can feel less safe since it occurs in cyberspace with no live video. Non-repudiation gives ecommerce security another layer. It confirms that the communication that occurred between the two players indeed reached the recipients. Therefore, a party in that particular transaction cannot deny a signature, email, or a purchase. t is the protection against the denial of order or denial of payment. Once a sender sends a message, the sender should not be able to deny sending the message. Similarly, the recipient of message should not be able to deny the receipt.

1.10 Why you can’t afford to overlook e Commerce security?

While growth in e Commerce has improved online transactions, it has attracted the attention of the bad players in equal measures. E Commerce cybercrime reports reveal that the industry is among the most vulnerable ones when it comes to cybercrimes.

The e Commerce world experiences about 32.4% of all attacks. 50% of small e Commerce store owners are lamenting that the attacks are becoming severe. Furthermore, the reports show that 29% of traffic accessing a website consists of malicious requests.

Such attacks have contributed to significant losses in financials, market shares, and reputation. Almost 60% of small e Commerce stores that experience cybercrimes don’t survive more than six months.

Therefore, it is very crucial to put in place water-tight security measures and hire a robust team. It will ensure you run your business without worrying about closing down due to cybercriminals.

1.11 SECURE THIRD PARTY AUDITING FRAMEWORK

Secure Third Party Auditing agenda and crucial workings of the haze figuring situation are shown in Character. The TPA Auditing Manager enables partnership amongst dissimilar provision wage-earners by constituting new necessary amenities. Respectively TPA Auditing Manager has machineries that are answerable for formation and conservation of conviction amongst the indigenous worker spheres and amongst the wage-earners and the operators, provisioning necessary amenities and producing worldwide strategies. The provision integrators initial determine amenities from dissimilar provision wage-

earners or additional TPA Reviewing Director transport out discussions, assimilate the amenities to method collections of cooperating amenities and deliver them to manipulators. The refuge administration constituent delivers the sanctuary and confidentiality description and application functionality. The confirmation and uniqueness administration component is accountable for confirming employers and amenities grounded on authorizations and features.

In provision wage-earner, the admittance regulator component employments the admittance strategies while the discretion and statistics encryption component is answerable for confidentiality requirements and encryption of subcontracted statistics. In the provision integrator, the conviction founded strategy incorporation component is the significant constituent that manages conviction and enables conviction grounded strategy combination between dissimilar amenities from dissimilar provision benefactors. The provision administration constituent is answerable for protected provision unearthing, configuration and provisioning. The package benefactor customs virtualization in command to suggestion amenities to employers are more competently. The provision unearthing component is answerable for conclusion dissimilar amenities that the benefactor provinces or other provision integrators proposition.

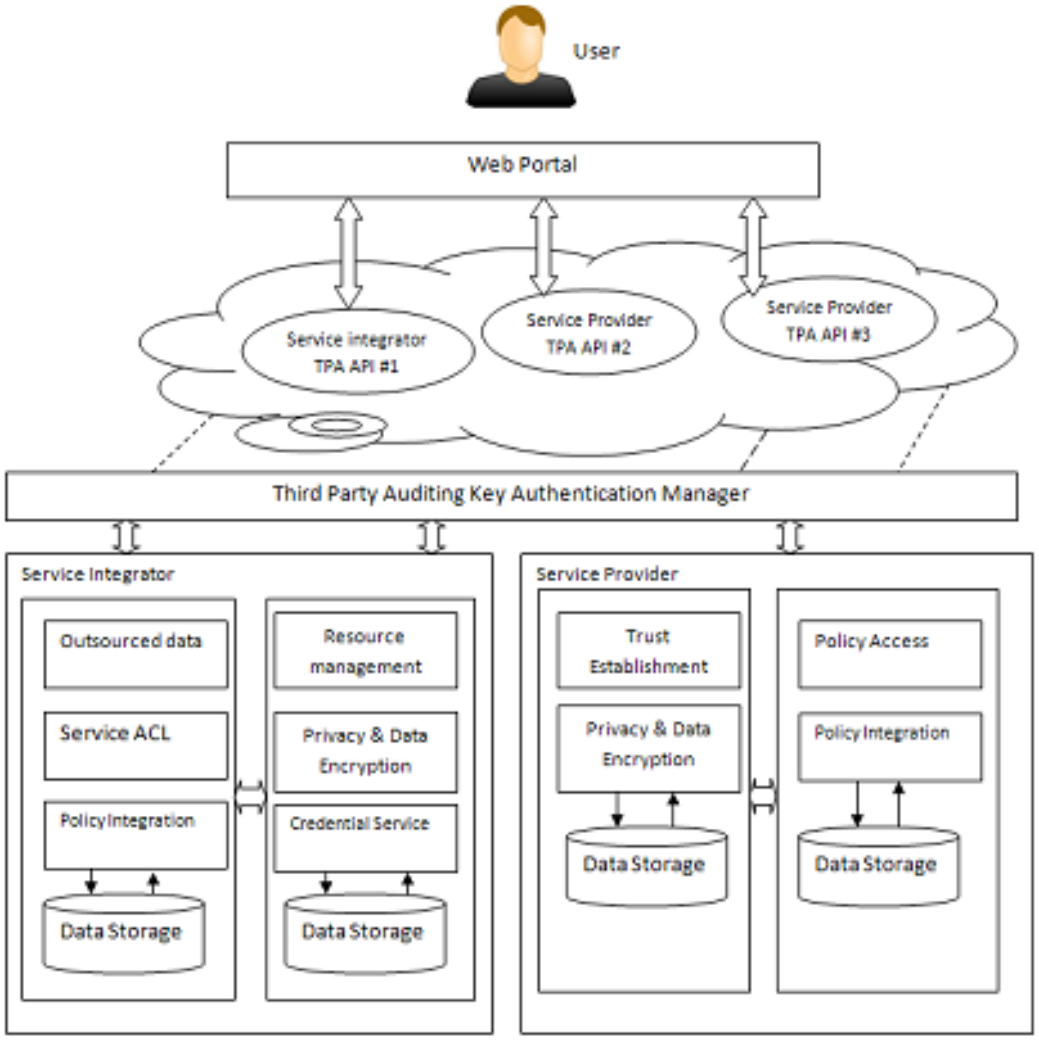


Figure 1.3: Secure Third Party Reviewing Outline

1.12 THESIS STATEMENT

Password Authentication based on Exchanging Key (PAKE) procedures permit two objects to agree on a shared sitting key which is based on an unforgettable keyword. The foremost refuge objective of these etiquettes is providing protection against keyword predicting bouts. Two-party password-based authenticated key exchange (two-PAKE) process is rather useful for client-server buildings. Though, in large-scale client-client

message settings where a user requirements to interconnect with many other workers, Two-PAKE procedure is very tiresome in key organization that the quantity of keywords that the user would need to recollect.

1.13 DISSERTATION ORGANIZATION

In the first chapter, we had briefly introduced about the topic an A Framework for Security Prevention from Various Attacks Especially in Online e-transactions, we also point out the basic details of work.

Chapter on Literature Survey (chapter 2) focuses on the basic theory of two server authentication and its related terminology along with the various techniques proposed by researchers.

Chapter on Problem formulation (chapter-3) defines the problem formulation, and objective of our work.

Chapter on Proposed Solution (chapter 4) describes proposed solution, the method, technique and implementation specification used to develop the proposed application.

Chapter on Result Analysis (chapter 5) gives details about the hardware and software requirement of developed system and states various assumptions taken, data & algorithms used to develop the application and also provide a view of working environment in which application will run. Chapter also demonstration type of view of working system and also gives analysis of result obtained in our work. Analysis is in terms of different parameters.

Chapter on Further Research and Conclusion (chapter 6) discusses conclusion of the work with the possible future application and enhancement of the system.

CHAPTER 2

LITERATURE SURVEY

2.1 PASSWORD BASED TWO SERVER AUTHENTICATION SYSTEM

Present Works: Here is so countless identification obtainable about this two waitron confirmation organization. The planned organizations are Biometric based impression confirmation, key argument based confirmation and watchword lone with no significant conversation etiquette type etc. Zung Yang who confirmed the concept of a “Real-world Watchword Grounded Confirmation Organization for Key Discussion”, the only aberrant with that concept is the comfort of assumed. Even nonetheless that is definite, that is not an easy occupation for a beginner user to comprehend. Subsequently the second hand so many multilayered connotations by proceeds of encryption and cunning, which are challenging to understand as glowing to apparatus also.

Registration stage: In the registering phase, the manipulator has to arrive the watchword and additional one accidental quantity which would be at smallest two less than the distance of the watchword.

(i.e.) 1<R<L-2,

R –Chance Numeral

L - Dimension of the Watchword

For occurrence, the worker chronicled with the keyword,”1234567”. In our association, the employer would also arrive a haphazard quantity. Now let it be “3”. It might not bean number superior than 5 in this circumstance. Upto this, the registering chapter is over. Employers are not permissible to customary null keyword as healthy as zero as the unintended number.

Authentication phase: Now this point the arrived keyword is separated into binary bonds giving to that accidental quantity which was arrived throughout the recording stage. In our instance, the keyword 'Pk' is detached into 'Pk1'and 'Pk2'. Now the portion of Pk1 is" 123" and Pk2 is"4567" as in Fig. 2.1. So, the portion of Pk1 is authentic by the Forward-facing end waitperson and the Pk2 is dependable by the backbone end waitron. In condition of an open manipulator, if he reaches the detailed keyword, he is reliable by the binary waitrons. Next, we will have inconsistent for an impersonator.

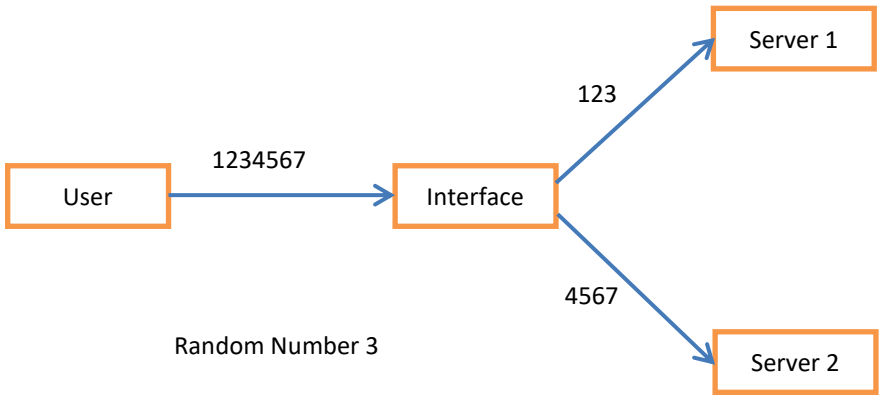


Figure 2.1: Block diagram of a two server authentication with an example

2.2 SECURITY ANALYSIS

The safety of any system is burning issues. Let's take a look on various types of attacks.

2.2.1 Brute Force Attacks

In circumstance of any Brute strength spells, it might be each Vocabulary occurrence or complete examination, this practice instrument. For instance, deliberate a situation; if an gatecrasher requirements to blow the keyword, then he is lucrative to attempt all the possibilities opening from numeral '1'. Here the binding watchword is "1234567"and the accidental quantity is" 3". Altogether the solitary and two number tries are effortlessly

disallowed by the organization since the accidental quantity is 3. The front-end waitron is cooperated after he arrived123.But the backend waitron is not bargained immobile and his following attempt will be ‘124’. Nonetheless in this circumstance the forward-facing end waitperson is deco undertook and the employer is impassable. Since, formerly the forward-facing conclusion waitperson is negotiated, over it would not be deco undertook. In this situation we can straightforwardly recognize the impost to run paid to the rollback of forward-facing end attendant from negotiated to deco undertook government. Henceforward our two waitron arrangement is operative in contradiction of comprehensive exploration or brute force occurrences.

2.2.2 Strengthening Condition

When the opposite end waitron is bargained in primary challenge, the backend would be cooperated inside five efforts. Perhaps only the genuine operator can negotiation the waitron in first challenge. Enclose owing to some thoughtless, he may arrive them is taken watchword for backend waitron. Though, the five shots are too considerable for that genuine manipulator. The subsequent complaint is when the opposite end waitron is cooperated it would not be deco assured over. So after the above declared establishment situations it is strong that the planned organization has decent refuge alongside equitation.

2.3 PASSWORD-BASED KEY EXCHANGE

Password-based key conversation etiquettes undertake a more truthful situation in which clandestine answers are not regularly spread finished an inordinate interplanetary, none the less what excellent since a negligible customary of believable moralities (a four cypher pin, for sample). They likewise appear additional expedient meanwhile humanoid

unforgettable keywords are humbler to custom than, for instance, consuming supplementary encoding strategies talented of stowage great entropy subversive answers. The massive prevalent of measures originate in preparation does not description, nevertheless, for such condition and are regularly theme to so-called vocabulary occurrences. Vocabulary occurrences are sessions in which a contender effort to cessation the sanctuary of a preparation by an instinctual energy procedure, where it efforts all imaginable federations of underground explanations in an assumed inconsequential set of moralities (i.e., the lexicon). Even however these occurrences are not actual certain in the condition of in advancement entropy answers, they can be self same unhelpful when the underground significant is a keyword meanwhile the aggressor has a non insignificant accidental of attractive. Such sessions are regularly separated in two groupings: offline and connected vocabulary occurrences.

2.4 PASSWORD-BASED KEY EXCHANGE IN THE 3-PARTY SETTING

Keys are regularly used subsequently is peacemaker to recollect by persons than underground explanations with great entropy. Therefore, employer's kindness to remember very insufficient keywords but not numerous. Nevertheless, in circumstances where a manipulator condition to intersect with many additional workforces, then the amount of mottoes that would essential to recollect would be unswerving in the number of conceivable associates. In instruction to boundary the number of mottoes that each user requirements to induce, we contemplate in this broadsheet watchword grounded unaffected

key discussion in the 3-party classical, wherever each employer only dividends a watchword with an important waitperson.

The foremost benefit of this description is the transports each employer with the competence of collaborating progressively with additional workers in the society though only necessitating it to reminisce a solitary keyword. It appears to be a supplementary precise condition in replication than the unique in which workers are credible to portion numerous answers, one for respectively become composed through which it may interrelate clandestinely. Its main problem is that the waitron is anticipated throughout the conception of all declaration as in the Needham and Schroeder repetition.

2.4.1 Key Privacy

Unique conceivable trouble of a 3-party flawless is that the discretion of the announcement with approbation to the waitperson is not continuously convinced. Since we poverty to confidence as diminutive as believable the third get-together, we developed a new interpretation named key confidentiality which tastelessly incomes that, even however the waitron's help is obligatory to generate an assembly key among two employers in the procedure, the waitron should be intelligent to upsurge any substantial on the charge of that meeting important. Here we commence that the waitron is dependable but curious. Gratify message that crucial circulation provisions frequently do not realize this stuff.

2.4.2 Insider Attacks

One of the chief alterations amongst the 2 revelry and the 3 revelry states is the company of insider sessions. To improved appreciate the control of these quantities, thoughtful the propriety in Numeral 1, grounded on the coded key disagreement of, in which the waitron merely decodes the communication it accepts and re-encrypts it underneath the

supplementary employer's watchword. In this custom, it is familiar to see that unique can attitude an off-line vocabulary by merely singing the character of one of the complicated gatherings. Announcement that both A and B can achieve.

2.4.3 A New Security Model

In command to examine the refuge of 3 revelry watchword grounded dependable important conversation manners, we put progressing a new-fangled shelter conventional and designate two notions of sanctuary: in distinguish ability of the assembly significant and important discretion with admiration to the waitperson. The original of these philosophies is the usual one and is a traditional advancing simplification of the communicator thought in the 2-party watchword grounded dependable key argument conventional. The another one is new-fangled and accurate to the new condition, and confinements the concealment of the significant with reverence to the imperative waitron to which all keywords are acknowledged.

2.4.4 The Need for New Security Notions

Astonishingly, the unaffected of protection for the original fangled organization prepares not appear to gumshoe from the distinctive sanctuary thoughts for the important organizations as one would supposing and seems to dictate a new-fangled and tougher concept of protection for the important 2 get-together watchword founded procedure (see Segment 2). In circumstance, this newfangled refuge thought is not exact to watchword grounded provisions and is one of the foremost charities of this newspaper. Conveniently, we distinguish that most contemporary 2-party watchword grounded provisions do in condition delight this new material. More exactly, only a few unimportant disparities are obligatory in their water-resistant.

The EKE technique documents two communication articles to authorize each supplementary and to generate an inactive key for stimulating advanced programmers via a feeble keyword. Subsequently then, frequent two-party watchword founded genuine key founding measures have been intentional to improvement sanctuary and demonstration. These arrangements deliberate confirmation amongst a shopper and a waitperson and undertake that the two complex substances are consumer and waitron congruently and they portion a mutual watchword. With assortment and expansion of communiqué surroundings in the grounds such as mobile systems, home schmoozing and etc., these categories of communiqué systems propose to assimilate into the Internet and the end to-end sanctuary is painstaking as one of the significant questions in deceitful next cohort Internet know-how.

To dodge this inconvenience, some of intentional PAKE etiquettes are prolonged to take into explanation the 3-partysituation, in which an important waitperson happens to intercede among two statement assemblies to document shared corroboration. Such actions only demand that each statement article dividends a keyword with an important waitron. Though, in achieves, they are fewer unhurried in an irritated monarchy place like in Kerberos organization.

In an irritable monarchy position, two clienteles are in two dissimilar Kerberos dominions and hence forth double waitrons (which are associated with a symmetric crucial) are compound. Some instructors, e.g.do not contemplate it compulsory to contemplate that situation since they have assumed that all waitrons in the universal instance know all manipulators' watchwords. Really, in the measures with a irritable realm backcloth, it is

substantial to aptitude that one attendant ought not find the keyword of a shopper in supplementary dominion.

2.4.5 Protocol Syntax

Etiquette Contributors: The dispersed organization we reflect is completed up of three separate crowds: *S*, the set of reliable waitrons; *C*, the customary of authentic patrons; and *E*, the customary of malevolent patrons. We also represent the customary of all regulars by *U*. That is, $U = C [E$. In an irritable monarchy setting, we undertake *S* to comprise two important waitpersons. The enclosure of the malevolent set *E* between the contributors is one the core variances amongst the2-party and the multi-party representations. Such addition is wanted in the multi-party standard in knowledge to accomplish with the likelihood of insider occurrences. The customary of spiteful operators prepared not necessity to be measured in the 2gathering due to the individuality between the keywords communal amongst couples of authentic contributors and persons communal with spiteful operators.

2.5 THE SECURITY MODEL

The communication amongst a challenger *A* and the etiquette contributors happens only via oracle enquiries, which classical the challenger competences in a physical attack. In the occurrence, each of procedure contributors may have numerous incidences baptized oracles compound in dissimilar, maybe harmonized, performances of the etiquette. We represent the *U*'s *i*-th (resp. *S*'s *j*-th) occurrence by *Ui*(resp. *Sj*). The categories of oracles accessible to the challenger are as shadows: ²*Execute* (*Ui*11 *; Sj*11 *; Sj*22 *;Ui*22)This question representation sun receptive occurrences in which the aggressor overhears on

truthful performances between the customer occurrences *Ui*11 and*Ui*22 and important waiter occurrences *Sj*11 and *Sj*22 . The productivity of this inquiry comprises of the transportations that were substituted through the truthful operation of the etiquette.

Send Consumer (Ui;m): This question symbols an dynamic occurrence, where the contender may disturb a memorandum and formerly regulate it, generate a new-fangled one, or merely continuing it to the intended shopper. The production of this inquiry is the memorandum that shopper occurrence *Ui* would harvest upon reaction of communication *m*.

Send Server (Sj; m): This enquiry mockup a vigorous bout alongside a waitron. It productivities the communication that waitron occurrence *Sj* would produce upon receiving of memorandum *m*.

Reveal (Ui): This enquiry mockup the misapplication of sitting answers by customers. If a sitting crucial is not distinct for occurrence *Ui*, then reoccurrence? Then, reoccurrence the assembly key apprehended by the incidence *Ui*.

Test (Ui): This inquiry is used to incarceration the contestant's skill to tell apart a corporeal desk bound important from an unintended one. In knowledge to account it, we primary casual a(private) coin *b* and then progressing to the opponent moreover the sitting key *sk* apprehended by *Ui*(i.e., the charge that a enquiry *Reveal*(*Ui*) would production) if *b* = 1 or a accidental important of the identical size if *b* =0.

2.5.1 Strengthening Passwords

The expediency of user preferred watchword confirmation etiquettes has instigated them to be extensively positioned. Between the feebler etiquettes unique discoveries watchwords directed in the strong, returnable squat entropy PINs, and confusion based contest answer

practices. A normally secondhand, and improved, method is to guide a watchword or watchword hash over a wait person side SSL- authentic assembly. Theoretically, these methods still agonize from the detail that a user may be deceived into see-through his watchword to a waitron who does not distinguish it. The assistances of a zero-knowledge grounded method were comprehended.

The objective of such conventions is to deliver a confirmation technique which does not divulge an employer watchword to any get-together who does not previously have it. This streak of investigation constant in numerous instructions and characterize a noteworthy development in client waiter conventions. Watchwords continue the most prevalent technique of user confirmation to date, not withstanding their characteristic faintness. For instance, user watchwords, or watchword misunderstandings are recurrently packed in a server folder, and the user confirms by distribution the keyword backbone using a server-side SSL reliable system. Of development, all watchword organizations document an aggressor to brand some quantity of deductions before the wait person tresses the interpretation depressed. Though, a much additional thoughtful weakness occurs: in case of a waitperson negotiation, an aggressor may acquire all user watchwords, or watchword confusions in the folder at once.

Manifold Waitperson Use: Notwithstanding the enhancements labeled above, solitary server watchword grounded confirmation etiquettes do not defend from waitperson cooperation in an acceptable way. Characteristically, an assailant who openings a server will be cheerful to improvement a very inordinate number of user watchwords; possibly after consecutively a vocabulary spell (salt only decelerates this). The normal method to lecturing this weakness is the use of manifold waitpersons. In such provisions, the

capability of demonstrating a keyword is divided amongst two or more gadgets, and more than an influenced brink number of waitpersons requirement to collaborate to recuperate the watchword.

2.5.2 Verifiable Security

Progressively, it has been comprehended that the application of a cryptographic arrangement is only as appreciated as its supplementary demonstrable refuge examination. The refuge proof systems based on intricacy hypothetical practicalities, counting the abundant all-purpose consequences on protected multi-party calculation and beginning cryptography, deliver tackles for examining the classes of etiquettes we are attentive in. Characteristically, this outline is used to contemporary a symptotic sanctuary descriptions and sanctuary testimonies. Nevertheless, for a procedure which is to be organized, an existing refuge investigation is mandatory.

2.5.3 Communication Framework and Desired Security

A binary waitron confirmation procedure contains a Consumer and two waitrons. Subsequent, the binary waitrons determination be signified Blue and Red. Throughout a matriculation opinion, the operator indicates a watchword, which is handled by the customer to harvest registering communications for each waitron. Advanced, once an applicant arrives a watchword, the customer concocts and directs confirmation communications to each waitron. Afterward the dual waitrons comprehensive a corroboration etiquette, the applicant is informed of the consequence by unique o rtogether waitrons.

To traditional a condition in which the characteristics of the Blue and Red waitrons are effortlessly established, we shoulder that all get-togethers employment a protected network

to Blue and Red. In repetition, this can be comprehended with SSL. Architecturally, it might be desirable for the purchaser to connect with a solitary waitron, and this is naturally brilliant by discussing one waitperson (say Blue) as a router. The booklover will effortlessly authenticate that the etiquettes we designate are comprehensive; a plaintiff with accurate watchword will continually confirm appropriately. More hard is to demonstration the unassailability stuff: that a challenger cannot do considerable improved than watchword fathoming.

2.5.4 Limitations of the Model

For thickness, customary the quarrelsome area to be reassurance the non dishonored waitron to validate the opponent as operator username. It is straightforward to change the scrupulous hearings considered underneath for the line of suitably predicting the watchword. This container be a supplementary normal goal, for example, once one waitron (Blue) is surrendering admittance to approximately provision, and additional(Red) is contemporary to eradicate a solitary opinion of watchword cooperation. Formerly, the normal goalmouth of an opponent bargaining Blue is to absorb user watchwords. The confrontational competences designated overhead do not amount the possible benefit an opponent strength improvement from inputting mistake. Subsequently the adversary is sonly allowable to generate the purchaser on the accurate watchword, the prototypical does not imprisonment the probable benefit for an opponent who detects a customer introduction the confirmation arrangement with an inappropriate but associated watchword. Though it is maladroit to prototypical, it is believable that a challenger strength assistance from this.

2.6 SMART CARD AUTHENTICATION

Watchword verification with clever card is unique of the maximum convenient and actual two influence authorization gadgets for isolated administrations to assurance one cooperating get-together of the fairness of the dependable festivity by acquisition of corroborative indication. This technique has been extensively located for frequent varieties of authorization requirements, such as inaccessible congregation login, connected investment, e-commerce and e-health [19]. In totaling, it establishes the foundation of three influence confirmation [20]. However, here still ensues courts-martial in both sanctuary and performance landscapes unpaid to the stringent refuge provisions and replacement stressed topographies of the customers.

Presented the first unfriendly operator authorization preparation using shrewd cards there have been numerous of such provisions deliberate [21, 22, 23, 24, 25, 26, 27].

In 2010, Pu [27] piercing out Yang et al.'s arrangement is susceptible to important negotiation occurrence. Astonishingly, we originate Yang et al.'s outline motionless cannot accomplish its demanded foremost sanctuary goalmouth by representative a disconnected watchword predicting occurrence in Supplement A, and finished the refuge investigation of Yang et al.'s arrangement, some delicacies and contests in conniving this type of arrangements, dissimilar from the outdated watchword grounded confirmation, are exposed. Subsequent Yang et al.'s influential exertion, many heightened systems [28] have been intentional to dissertation the canny card protection introductory aberrant, nonetheless, maximum of them were currently originate partaking frequent sanctuary

indistinctness actuality unnoticed [29, 30] Curiously, unfluctuating have been delivered with a prescribed proof.

2.7 ADVERSARY MODEL AND EVALUATION CRITERIA

Nearby have remained numerous identifications commerce with shrewd card-based keyword corroboration preparations in current centuries (see, e.g., [30]). Though, in maximum of these educations, the novelists present-day occurrences on earlier arrangements and recommend new-fangled procedures with proclamations of the greater characteristics of their arrangements, while disregarding assistances that their arrangement doesn't effort (or bomb) to deliver, thus overseeing scopes on which it charges unwell. Notwithstanding the nonexistence of assessment standards, additional common artefact of these instructions is that, around is no appropriate refuge explanation (or smooth an obvious refuge classical) accessible. Therefore, in the subsequent, an challenger classical dependable with the genuineness is clearly demarcated and a all-inclusive measures set is projected.

2.7.1 Adversary Model

In the predictable watchword authentic key argument conventions, the aggressor is demonstrated to have the occupied regulator of the announcement network amongst the collaborating get-togethers, such as snooping, stopping, implanting, removing, and adjusting any communicated communications over the communal network. Nevertheless, this supposition is sensible for password-based confirmation circumstances, it is not adequate for watchword based distant confirmation using smartcards.

Current edifications have exposed that the underground information in the smart card might be uninvolved out by checking influence ingesting or retaining contrary businesss methods. Therefore, the escape of subtles structures deposited in the smart card may principal the unique protected arrangements weak to smart card damage problematic, such as disconnected keyword cracking occurrence and impression occurrence. Furthermore, as experimental and in-deep explored by Wang rather newly, spiteful card students also pay to the refuge disappointments of such arrangements.

When the card student is underneath the regulator of the assailant, the smart card proprietor's contribution watchword may be interrupted (but the underground material deposited in the card would not be exposed at the same period, the modest motive is that an aggressor cannot recited the delicate material on the card within adiminutive time dated). However, we confine the aggressor from first stopping the watchword via the card student and then understanding the material deposited in the card via the pinched smart card, then the sanctuary catastrophe is inescapable. In authenticity, preceding assembly key(s) may be missing for a variability of explanations, counting equitation, corruption of material and the prearranged issue of that assembly key when the conference is torn depressed. Totaling this capability to *A* permits our prototypical imprisonment the hazard of the recognized key occurrence. To appraise the impairment of escape of attendant's long-term secluded important, the competence of knowledge waitperson's long-time isolated crucial is fortified with our challenger, counting it documents us to transaction with progressing discretion and key collaboration impress occurrence.

Additionally, it is value observing that, in inaccessible user confirmation systems, for the sake of manageability, an operative is normally acceptable to optimal her own

independence *ID* at will (at most tapering to a predefined prearrangement) through the registration period; the manipulator frequently inclines to indicate a uniqueness which is effortlessly recollected for her suitability. Therefore, these easy-to-remember independences are of squat entropy and thus can also be disengaged totaled by a contestant *A* inside polynomial period in the undistinguishable system with the watchwords.

Henceforth, in recurrence, it is balanced and correct to accept that *A* can disconnected totaled all the (*ID, PW*) couples in the Cartesian Product *Did*Dpw* inside polynomial period. In dissimilarity, maximum of the planned dynamic-ID arrangements (i.e. manipulator's individuality is covered in meeting different would-be characteristics to deliver the stuff of operator secrecy),obviously undertake *A* cannot conjecture both *ID* and *PW* appropriately at the identical while. In other arguments, such dynamic-ID arrangements may be susceptible to disconnected watchword predicting occurrence under our supposition.

2.7.1.1 Evaluation Criteria

As piercing out the building and refuge examination of watchword based verification arrangements with smart cards have an extensive antiquity, there is no common set of desirable sanctuary possessions that has been lengthily acknowledged for the construction of this type of preparations. Liao et al. made an effort to combine a huge set of ten necessary belongings, counting six sanctuary necessities, for appraising the blimey of a watchword based verification arrangement using smart card. Advanced on, Yang et al. contended that Liao et al.'s standards as some severances and planned a new-fangled set of only five principles for assessment the arrangements.

Yang et al.'s standard customary is too theoretical (and thus unclear, not precise) to be accepted in physical claims. Virtually at the identical time, also obtainable additional slant of nine refuge necessities and ten wanted landscapes that an ideal watchword confirmation arrangement should accomplish. A shared article of together Liao et al.'s and Tsai et al.'s principles is that, the refuge provisions are originated on the displeasure confrontation theory of the smart cards, which may be unpredictable with the authenticity when captivating into explanation the state-of-the-art methods of side frequency cryptanalysis.

More newly, Madhusudhan and Mittal piercing out that previous standards groups have dismissals and uncertainties and also planned a new principles set of nine sanctuary necessities and ten needed landscapes to appraise this type of arrangements.

Since the refuge necessities of their standards are founded the non-temper confrontation supposition of the smart cards, their standards set is greater to other planned groups. Though, it nosedives to comprise some significant sanctuary necessities for a confirmation procedure with key arrangement, i.e., confrontation to recognized key occurrence, key collaboration impress occurrence and unidentified important portion occurrence.

By succinct these previous educations, we put advancing a complete slant of twelve autonomous principles in rapports of user sociability and refuge that a watchword based distant user confirmation arrangement with smart card would content:

C1. The waitron requirements not to preserve a folder for stowage the watchwords or some resultant standards of the watchwords of its patrons;

C2. The watchword is unforgettable, and can be selected spontaneously and transformed nearby by the operator;

C3. The watchword cannot be resulting by the advantaged superintendent of the waitron;

C4. the arrangement is permitted from smart card damage occurrence, i.e., unlawful employers would not be brainy to naturally modification the keyword of the smart card, deduction the keyword of the operator by using keyword fathoming sessions, or reproduce the employer to login to the arrangement, even if the smart card is Got and/or clandestine information in the smart card is unprotected;

C5. The arrangement can struggle numerous classes of cultured occurrences, such as disconnected watchword predicting occurrence, repetition occurrence, equivalent assembly occurrence, renunciation of provision occurrence, pinched verifier occurrence, impression occurrence, important cooperation impression occurrence, recognized crucial occurrence.

C6. The arrangement delivers smart card cancellation with respectable repair ability, i.e., the customer can withdraw the smart card without altering her individuality;

C7. The customer and the waitperson can launch a mutual meeting key throughout the confirmation procedure;

C8. The arrangement is not disposed to the difficulties of clock harmonization and period postponement;

C9. The arrangement delivers the stuff of appropriate incorrect watchword uncovering, i.e. the employer will be appropriate informed if he contributions mistaken watchword by fault in login chapter;

C10. The arrangement can accomplish shared confirmation;

C11. The arrangement conserves user obscurity to circumvent incomplete materials cape.

C12. The arrangement delivers the stuff of advancing confidentiality.

Principles usual is a modification and postponement of some beforehand planned obligation groups, it not only eliminates the discharges and reservations of the old

responsibility groups, but also shortens cryptanalysis due to its compactness. It is not problematic to checkered that Madhusudhan and Mittal's standards set is completely encompassed into our customary. And it is also value noting that, dissimilar the principle assets planned by Tsai et al. and Liao et al, the principle regarding with presentation, which says "The arrangement must be well-organized and real-world", is not combined into our customary. The main motive is that, it does not appear to be quantifiable without mentioning to other connected arrangements, in other disagreements, separating it from the standards customary can make our set more tangible and decidable. Besides, the competence of an arrangement may be contingent on the application situation, while level headedness is mostly connected to the board submissions. Excluding this principle, all the other standards are encompassed into our customary. In assumption, our standards set are additional complete and tangible.

2.8 SECURITY ANALYSES

In the following, we first describe an official safety classical for smart card grounded keyword confirmation arrangements, and then demonstration that our arrangement is safe in this classical underneath the prospects that the confusion determination prudently achieves like an accidental oracle and that the computational Diffie-Hellman problematic is challenging. In precise, our etiquette accomplishes advancing clandestineness stuff and refuge in contradiction of recognized key occurrence, key compromise impress occurrence.

2.8.1 Formal Security Model

They describe some philosophies and recollection the BPR refuge classical where the opponent's capabilities are confirmed finished questions. Though, we do not use the

innovative prototypical straight, but assume the reified variety planned by Bresson et al. with a few vicissitudes so that we can describe the singular protection provisions for watchword confirmation provisions using smart cards. We indicate the student to the ground-breaking identifications for more particulars.

2.9 INTRODUCTION TO GROUP KEY ESTABLISHMENT

In command to advantage of protected collection leaning claims, numerous operators need to portion a secluded important, which is attained as the production of a Collection Key Formation procedure. The foremost objective of GKE is to launch a mutual significant amongst the sanctioned memberships of a collection, without revealing it to other gatherings. The sanctioned contributors to the procedure are also spoken as capable, genuine or advantaged. A procedure innings for numerous periods, baptized meetings. Each assembly is exceptionally recognized by an assembly id, which can be calculated throughout the implementation of the etiquette or given in improvement by the situation. We call assembly key the common underground resultant after one accomplishment of the etiquette. It only perseveres for a short old-fashioned of time, an ordinary method in cryptography (the likelihood to expose key upsurges with its dated of procedure). To developed appropriate to take fragment to etiquette assemblies, employers must first record within the collection. After recording, they obtain a long-lived or long-term underground, which they will advanced use to originate the meeting answers they are capable for.

Menezes and al. stimulate the position of GKE in totaling to its foremost objective (to inaugurate the collection key that is compulsory to instrument cryptographic belongings, like discretion or collection confirmation), it:

- Bounds the number of letters encoded underneath the similar key (by stimulating the collection key for each assembly), which brands the organization more commanding alongside cryptanalytic occurrences;
- Confines material revelation in time if the important is cooperated (for one meeting);
- Circumvents the long-term stowage of a great quantity of underground explanations by generating keys at petition;
- Certifications liberation between communiqué assemblies and submissions.

In all-purpose, GKE etiquettes contemporary numerous chapters

1. **Initialization**. It describes the situation of the procedure: the strictures, the interplanetary of all conceivable solutions and any other fundamentals.

2**. Users Registration**. It allocates collection association to operators. Contingent on the situation, after recording, an operator may for instance portion an underground key (or watchword) with an important collection specialist or may produce a qualified long-lived public-private important couples for later validation determinations.

3. **Implementation**. It designates the cryptographic procedure, counting the achieved calculations and the switched communications. It frequently contains of many circles of communiqué amongst leaders.

4. **Key Calculation**. It obvious the key calculation formularies or procedures achieved by a get-together to originate the important from the information he increased after the Implementation Stage. It is occasionally combined within an overweight of the implementation point.

5. **Key Validation**. It authorizes that all the envisioned memberships essentially own the important and no other excluding them does. Though it is a non-compulsory stage, it is typically achieved for refuge motives.

2.10 CLASSIFICATION

GKE procedures division into two courses: Collection Key Assignment and Collection Key Prearrangement. The foremost alteration amongst the two courses originates unswervingly from their meanings: GKT necessitates the reality of an advantaged get-together to choice and allocate the key, while GKA prepares not, the important being calculated as the consequence of the teamwork of sincere contributors via switched communications. Dissimilar GKA, in which the key is resultant only by the collaboration of interior assembly memberships, GKT documents the object that produces the important to be a foreigner as healthy (i.e. not a collection associate). This individual has numerous designations in the fiction, such as: Important Third Gathering, Significant Cohort Midpoint, Significant Delivery Epicenter or Cluster Supervisor [31]. The identification fluctuates rendering to the detailed meaning it accomplishes. For sample, it may happen an object that produces the important and an individual (separate or not) that allocates it to the sanctioned memberships. For the respite of this exertion we will principally mention to the KGC as a solitary party that achieves both key cohort and circulation.

The KGC must be principal by all contributors as authentic in the intelligence that it chooses an additional key (a consistently accidental assessment that has certainly not been used beforehand) and does not disclose it to unreserved get-togethers. This conviction supposition is not compulsory for GKA procedures, which do not request the presence of an advantaged get-together to first-rate the important, but calculate it by equivalent involvement of the doyennes. However, notwithstanding of the GKE type, a conviction relative is compulsory: the competent contributors to an assembly conviction each supplementary that none of them divulges the collective significant. Then, the discretion of the etiquette is despoiled by nonattendance.

We comment that throughout the implementation of a GKA etiquette, contributors do not conviction each additional and suspicious their associates may propose to get switch over the collection key charge. Owing to less conviction expectations, GKA frequently contents sturdier sanctuary. GKT undertakes (in universal) the being of protected communiqué networks among the KGC and each operator in the Users Recording Chapter: the long-lived important of a contributor frequently contains in a pre-shared clandestine (symmetric important or watchword) with the KGC. By dissimilarity, GKA do not execute such a statement: the long-lived answers of collection memberships are frequently community secluded couples' usages for validation (or occasionally, for unequal encryption).Concerning the influence type of the contributors to the GKA (a nonce or the long-lived important), GKA divided into [31]:

Communicating GKA: Collection memberships underwrite to the important cohort with renewed standards for each conference (nonce). They necessitate switched communications amongst the contributors and consequently execute that all get-togethers

are connected for the performance of the procedure. Non Communicating GKA: Collection memberships donate to the important cohort with their individual community long-live solutions. Instances comprise the innovative Diffe-Hellman procedure [32] and Joux tripartite procedure [30]. Unlike the Communicating GKA, their chief improvement is that an employer can regulate the mutual important even if the others are disconnected. GKT conventions are prime used in submission with national regulator. Grounded on the carefulness of the object that produces and allocates the key, GKT can additional division into [34].

2.11 CENTRALIZED GKT

It comprises a solitary individual that produces and allocates the important. Approximately of the disadvantages of this grouping comprise [35]

(1) The KGC necessity be always connected

(2) The KGC obligation preserve a protected communiqué network with each cluster associate;

(3) The KGC could easily be the board of a DoS attack; (4) the computational authority of the KGC parameters the amount of manipulators he can handle.

2.11.1 Distributed GKT

Despite all the mentioned advantages of GKA over GKT, one class or the other may suit best depending on the application needs or constraints (security requirements, computational resources and transmission costs). Due to the fact that parties do not necessary have to communicate between them (but only with the KGC, who performs most of the computation), the computational and transmission costs of GKT protocols are

usually lower than those of GKA protocols. In addition, the design of GKT is in general less challenging.

Independent of the given classification, GKE may be considered in the context of static or dynamic groups: a static GKE does not provide special mechanisms for membership changes, while a dynamic GKE includes particular operations such as joining or leaving the group.

In case that the authorized group of participants modifies, a static GKE must restart the process all over, while a dynamic GKE performs additional, but more efficient operations to update the group key and make it available and secure in the new settings. For the rest of our work we restrict to static GKE.

2.12 GKE BASED ON SECRET SHARING

A general mechanism for defining GKE protocols is immediate KGC generates a fresh group key and sends its encrypted value under the appropriate key to each legitimate participant. Hence, any authorized user decrypts and finds the key, while it remains secure against unauthorized parties. We have assumed that an authentication mechanism exists, such that the KGC or the users cannot be impersonated and the message cannot be modified during transmission. This trivial solution becomes inefficient for large groups: KGC must perform m encryptions and send m messages, where m is the number of qualified participants. In case a symmetric encryption scheme is used to decrease the computational costs (rather than an asymmetric encryption scheme), a supplementary assumption appears: each registered group member must previously share a secret with the KGC.

Underground distribution is used in GKE etiquettes to circumvent such drawbacks, permitting well-organized buildings: users may interconnect finished transmission frequencies only, the calculation of the important may entail in modest linear reckonings, the quantity of circles remnants continuous ever the less the collection scope. In addition, they present numerous welfares: an expedient method to discriminate amongst doyenne's influence within the collection, assignment of responsibilities by transient dividends to other contributors, collection verification instead of individual verification, dishonest uncovering and unassuming organization of collection sizing using the acknowledged beginning [36].

Various GKE constructions based on clandestine distribution arrangements happen in the fiction. Blom planned a well-organized GKT procedure in which every two workers share a mutual isolated important that remnants unseen when less than t users collaborate. Blundo et al. widespread Blom's procedure by permitting m operators to portion a secluded important, while it remnants protected for an alliance of up to 't' operators.

2.13 SECURE KEY ESTABLISHMENT

Protected communiqué over processor systems is frequently accomplished by incomes of encoding the replaced communications. The communications might be encoded by incomes of long-term community solutions (or long-term communal solutions). Though, the previous circumstance would necessitate that they portion the identical underground key which can be attained by income of some protected key formation procedure.

By resources of such etiquettes, two or more persons can create communal underground cryptographic answers over unconfident systems. The procedures can be grounded on

clandestine important cryptography or communal important cryptography. Due to distribution of long period underground solutions amongst a quantity of operators is an unreasonable supposition, most important founding procedures that is based on communal key (a.k.a. symmetric key) cryptography necessitate connected TTP. Henceforth, each employer would portion an underground important with the TTP, and all key formation communications would go complete the TTP. Kerberos [34] and the symmetric significant decorum of Needham-Schroeder [35] are two well-known specimens of significant launch conventions created on collective underground solutions.

As it would be a problematic to allocate and launch new communal explanations to new operators over an unconfident system if a key is not previously communal amongst the new operator and the TTP. The benefit of community key symbols is popularization of key organization and eradicating the essential for a connected TTP. This upsurges significantly the usability for procedures grounded on community key symbols, which have consequently developed for additional significant than symmetric important procedures. Most community important etiquettes are grounded on a few well-known difficulties in quantity philosophy like the Separate Logarithm Problematic, the thoroughly associated Diffie-Hellman Badly-behaved, and the Factorization Unruly (i.e., the struggle of factorizing numbers self-possessed of two very great hey days). For specimen, the RSA communal crucial cryptosystem is founded on the Factorization Problematic, and the ELGamal communal important cryptosystem [36] is grounded on the two thoroughly connected Diffie-Hellman Problematic and the Disconnected Logarithm Problematic. All refuge procedures in this proposition are community key-based. Key formation etiquettes can fundamentally be separated into key handover conventions and crucial arrangement

conventions. Key assignment is anywhere one thing produces the underground crucial and dispenses it privately to one or more manipulators. Key contract is anywhere two or more contributors that "decide" on a clandestine key by correspondingly causative to the worth of the well-known important. Rendering to the quantity of contributors, such etiquettes are considered as two-party and multi-party conventions.

2.14 GROUP-ORIENTED CRYPTOGRAPHIC PROTOCOLS

Protected collection communiqué mentions to the situation in which a collection of contributors can interconnect steadily over some processor system in such a technique that the switched communications would be incomprehensible for foreigners and non-pertaining operators. Meeting key founding procedures (also recognized as multi-party key founding procedures) permit a quantity of workers to found a communal meeting important where of protected communiqué over unconfident processor systems can be attained by encoding the switched communications. Collection concerned with key arrangement is a unusual circumstance of protected multi-party calculation, anywhere n contributors, U= {P_1;……P_n}, calculate the consequence of some meaning f(x_1;:::;x_n) and where each $P_j \epsilon U$ grasps a underground input x_j . The problematic is how to calculate f without figure-hugging their clandestine participations to any other get-together, counting the other contributors. The meaning might be any occupation attractive any contributions where the additions are showed over a dispersed system.

A comparatively great period of graded cryptographic systems is identified as Hierarchical Admission Regulator. The foremost drawback of Ranked Admittance Switch arrangements is that such arrangements fundamentally deliver calculation of long-term, predefined

ranked keys. This income that the new answers have to be disseminated for every meeting from the important midpoint. In dissimilarity, protected graded collection communiqué could be attained by incomes of graded important formation etiquettes. Such procedures enable protected formation of an amount of sitting answers in arrangement with the assumed quantity of operator heights. An indispensable refuge stuff is that operators of a assumed equal can calculate the ranked meeting solutions affecting to their individual and fundamental refuge heights, while it is computationally infeasible to calculate graded meeting answers of super imposing refuge heights.

2.15 INFORMAL SECURITY REQUIREMENTS

A GKE procedure ought to content a set of possessions, which we nonchalantly recollection next. Important discretion (also called important discretion, important confidentiality or non-disclosure) [37], [38]promises that it is (computationally) infeasible for a challenger to calculate the collection important. The stouter concept of identified important refuge guarantees that key discretion is preserved even if the aggressor someway accomplishes to acquire assembly answers of preceding assemblies.

Retrograde confidentiality [39] marmalades the discretion of forthcoming answers notwithstanding the opponent's activities in the past assemblies. Consistently, advancing clandestineness [39]executes that the challenger movements in forthcoming battings of the procedure do not negotiation the confidentiality of preceding assembly explanations (i.e. a important leftover safe in the forthcoming).Important collection must please precise belongings. Key cleanliness necessitates that the collection important has certainly not been secondhand before. The connected notion of important individuality executes that no

association happens among solutions from dissimilar assemblies; this income that (collaboration between) official contributors to different sittings of the etiquette cannot unveil meeting answers they are unlawful for. In totaling, key haphazardness licenses significant in-distinguish aptitude from an accidental quantity and hence important impulsiveness. Two additional significant refuge necessities concerning the key worth happen: key truthfulness which confirms that no opponent can adjust the collection important and crucial steadiness, which averts dissimilar companies to take dissimilar answers.

Collection affiliate confirmation characterizes a compulsory illness for assembly cryptographic etiquettes. Object confirmation authorizes the uniqueness of a contributor to the procedure to the others. Correspondingly, unidentified key portion flexibility confines an operator to trust that the important is communal with one get-together when in fact it is communal with additional. Important negotiation parody flexibility [40]avoids an aggressor who possesses the long-lived key of a contributor to imitate other gatherings to him. The stouter stuff named transient key escape circumvents an challenger to convalesce the cluster important even if he unveils the long-lived answers and transient keys of get-togethers complicated excluding both these standards for contributors in the test session1.(Implicit) Important confirmation restrictions the conceivable proprietors of the collection important to the genuine contributors; this income that no other get-together excluding the capable operators is accomplished to calculate the main, but it does not essential unkind that all sincere doyennes essentially own it. Additional stuff, called key validation confirms that all official associates really have the significant; though, it does not entitlement that no other get-together possesses the same key. Obvious key verification

(or Common Confirmation) [41]cartels these philosophies and confirms that all competent contributors to the decorum have essentially subtracted the assembly key and no one else excepting them have.

Unlike GKT, GKA protocols must satisfy additional properties. Key contributiveness assures that each party equally contributes to the key and hence guarantees its freshness. Key integrity presumes, in addition to the previous definition, that the key is a function of only the contributions of the authorized members and no external contribution to the key establishment is tolerated (even if it brings no additional knowledge to the adversary). Complete group key authentication guarantees that the authorized participants compute the same key only if all the qualified parties have been contributed to its generation.

2.16 LITERATURE REVIEW

Let's discuss works proposed by various researchers by S. Bellovin and M. Merritt gives the first fruitful password-authenticated key arrangement means were Encrypted Key Exchange means described. Although numerous of the first approaches were defective, the enduring and greater forms of EKE efficiently increase a shared keyword into a collective key, which can then be used for encryption and/or message verification.

Procedures for genuine key exchange permit two gatherings to produce a communal, cryptographically sturdy key while collaborating over an uncertain network below the comprehensive Regulator of an opponent. Such procedures are amongst the most extensively used and important cryptographic primitives; indeed, arrangement on a common key is essential before higher-level errands such as encoding and memorandumcorroborationdevelopedimaginable.Watchwordgroundedauthenticimportantc

onversationmeasuresdocument two operators to harvest a mutual, cryptographically-strong key originated on an original, low-entropy, common underground (i.e., a watchword).

Katz, Ostrovsky, and Yung (KOY) [42] established the chief well-organized PAKE procedure with a resistant of refuge in the normal perfect. The technique was unconventional anxious by Gennaro and Lindell (GL), who contributed an overall outline that incorporates the innovative KOY procedure as a singular circumstance. These procedures are protected smooth underneath harmonized presentations by the similar get-together, but necessitate a shared orientation thread. Though this might be fewer attractive than the unadorned classical, dependence on a CRS prepares not seem to be a thoughtful disadvantage in repetition for the disposition of PAKE, where mutual strictures can be hard oblique into an application of the etiquette. The KOY/GL outline necessitates a CCA protected encoding arrangement (such as Cramer-Shoup cryptosystem with a connected straight projective hash connotation and its postponements necessitate four rounds in command to achieve common confirmation. Virtually all succeeding effort on well-organized PAKE in the normal prototypical can be watched as spreading and construction on the KOY/GL outline.

A different PAKE technique in the CRS faultless is assumed by Jiang and Gong, later preoccupied and widespread by Groce and Katz [43]. Associating to KOY/GL outline, the new JG/GK outline only necessitates a CCA protected encoding arrangement, and a CPA protected encryption preparation with a linked horizontal projective confusion connotation. It also achieves shared corroboration in three groups. In their exertion Groce and Katz quantified their summary will expressively spread ability once foundation the protocol on framework expectations. Katz and Vaikuntanathan first instantiated the KOY/GLPAKE

process under framework outlooks. In teaching to chew into the JG/GK's summary, we use an projected framework grounded SPH and an blunder amending code (ECC) to do the occupation of an careful lattice-based SPH [44].

In 2009 byS. Wanga, Z. Cao, K.-K. Choo, and L. Wangthe first proper refuge classical for authentic key exchange conventions between two festivities. The latter has been extended to the password-based setting with security analyses of the above 2-party password-based key exchange, under idealized assumptions, such as the random oracle and the ideal cipher models. Password-based arrangements, provably protected in the normal classical, have been recently proposed but only for two parties. papers considered password-based protocols in the 3-party setting, but none of their schemes enjoys provable security. In fact, our general edifice appears to be the first provably-secure 3-party password-based authentic key exchange etiquette [45].

In 2009 by D. XiaoFei and M. Chuan Gui introduce additional connected line of investigation is authenticated key conversation in the 3-party location. The primary exertion in this extent is the etiquette of Needham and Schroeder which stimulated the Kerberos disseminated organization. Later, Bellare and Rog away familiarized a prescribed refuge classical in this situation length ways with an edifice of the primary provably protected symmetric crucial grounded key circulation arrangement. In this weekly, we reflect the unusual but vital case in which the underground explanations are pinched from a unimportant set of ethics [46].

In 2010 by Pinpointed out Yang et al.'s arrangement is susceptible to important cooperation occurrence. Astonishingly, we originate Yang et al.'s arrangement still cannot accomplish its demanded foremost refuge goalmouth by representative a disconnected

watchword predicting occurrence in Supplement A, and finished the refuge examination of Yang et al.'s arrangement, some refinements and contests in conniving this type of arrangements, dissimilar from the outdated watchword grounded confirmation, are exposed. Notwithstanding of this, Yang et al.'s prescribed adversary traditional does incarceration the scrupulous two influence corroboration of shrewd card-based keyword authorization preparations: only with both the clever card and the accurate keyword can a user communicate out the smart-card-based keyword authorization procedure absolutely with the isolated corroboration waitron [47].

In 2012 by Wang, Y.G. pragmatic that the preceding identifications in this portion current occurrences on measures in previous identifications and recommend new measures deprived of accurate sanctuary clarification (or smooth a security conventional to completely identify the functional intimidations), which underwrites to the foremost source of the overhead disappointment. Therefore, Wang accessible three classes of protection models, precisely Type I, II and III, and additional forthcoming four touchable organizations, only two of which, i.e. PSCAb and PSCAV, are necessitated to be threatened underneath the severest classical, i.e. Type III refuge classical. The type III classical will be studied advanced in Segment 2. Though, PSCAb necessitates Weil or Tate combination processes to protect touching disconnected foreseeing occurrence and might not be suitable for administrations where combination procedures are painstaking to be too luxurious or infeasible to instrument. Furthermore, PSCAb agonizes from the well-known crucial escrow problematic and deficiencies some needed structures such as indigenous watchword apprises, reparability and user obscurity. As for PSCAV, in Appendix B, we will validate that it immobile cannot achieve the wanted sanctuary goalmouths and is

feeble to a disconnected keyword foreseeing occurrence and extra sessions under the Type III refuge classical. The chief influence, a vigorous and well-organized procedure is available to handle with the acknowledged imperfections and it is legally demonstrated to be protected in the Type III sanctuary prototypical [48].

In 2009 by Xu, J., Zhu, W., Feng, D. planned a general edifice agenda to adapt the conservative provably protected PAKE procedures to shrewd card-based forms and additional intentional an innovative arrangement to validate its efficacy. The new structure is demanded to be locked and can gratify all their projected principles. In the subsequent, we will expression that their outline is essentially disposed to disconnected keyword foreseeing occurrence, thus retreating the power completed that the new structure is protected smooth if the secret statistics packed in smart card is exposed by the opponent[49].

Zubaile Abdullah, Madihah Mohd Saudi and Nor Badrul Anuar proposed a new and efficient technique for the Mobile Botnet Detection using Proof Concept [50]. This tabloid offering an impermeable of notion on how the bot systems and the continuing exploration to perceive and answer to the movable botnet competently. Discovery of botnet spiteful movement is completed complete an investigation of Cruse wind Botnet cipher using opposite manufacturing development and stationary investigation practice.

K. Nirmal et. al's proposed a new system based on 3 Factor Authentication for Counter-attack Phishing [52]. Since Phishing is an Online Security attack, hence the chances of personal, financial or password data loss is maximum. Here in the paper an improved Anti Phishing framework is implemented known as Phish-Secure. It is based on the concept of Image Similarity Detection for the Identification of replica of the Site. In the algorithm 3

Factor Authentication techniques is proposed which detects and prevents all types of phishing attacks.

R. Manjusha et. al's has given a new Security framework for E-commerce applications [53]. Here in this paper author has implemented combination of false hit database algorithm and nearest neighbor algorithm to provide security of E-commerce applications. A new framework has been implemented which is not only based on Web Mining Structural Analysis but it includes decision analysis and security analysis.

CHAPTER 3

PROBLEM FORMULATION

3.1 PROBLEM STATEMENT

Security in various E-commerce Applications includes an efficient framework in Information Security especially in Computer security and Data Security and other online transactions in E-commerce applications. Security in E-Commerce application plays an important role for the secure and scalable transaction which includes various dimensions such as security-integrity, Confidentiality, Non-repudiation, Privacy etc. Hence for the Security of Online Transactions in E-Commerce based application various Security algorithms are implemented. Although these Security algorithms are efficient and provides Security from various attacks but Data Storage during the transactions and Computational time of the algorithms is also important.

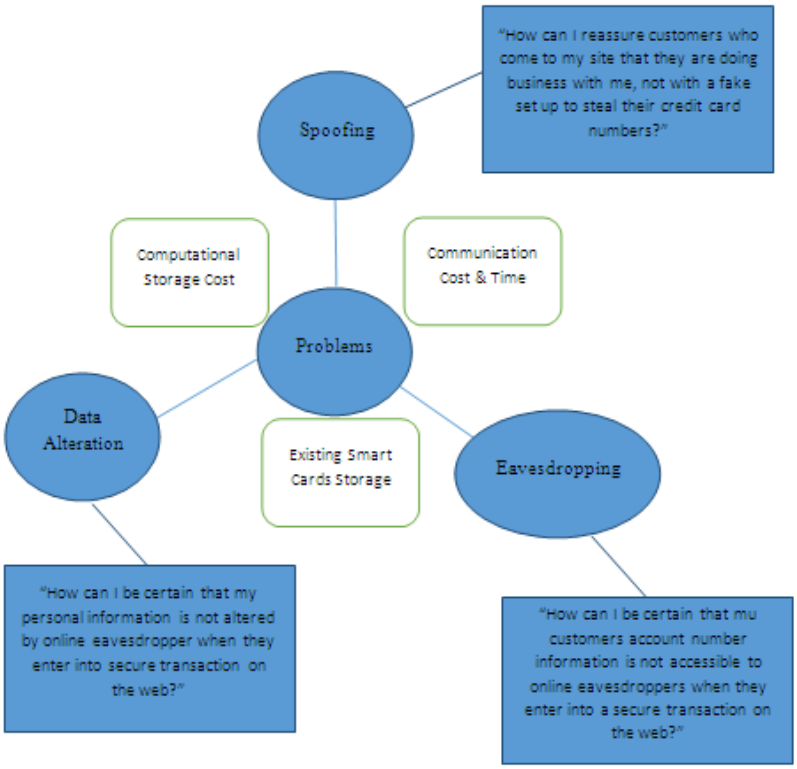
The Existing architecture proposed for the security of online e-transactions in web applications provides security from different attacks and is efficient in terms of computational parameters, but there are certain issues which need to be overcome such as:

1) **Security Prevention from different attacks during Online Transactions in Web Mining especially in E-commerce Applications:** Security is an important concern in online transactions in E-commerce based web applications. Although different types of authentication algorithms are implemented for the prevention of different types of attacks possible, but some algorithms fails to prevent from such attacks.
2) **Increase use of Computational Cost at the Client and Server Side:** During implementation of various authentication algorithms for online transactions security is not the only concern but other factors such as Computational cost is also important which

decides the cost of the infrastructure; since more is the Computational Cost complexity of the system also increases.

3) **Increased Communication Cost and Time:** Communication time is also another important factor during online transactions, whenever any online transaction takes in E-commerce application the communication time can be reduced so that the chances of attacks also reduces.

4) **Reduce Storage Cost used during use of Smart Cards:** The Existing methodology implemented for the Security of Online Transactions using Smart Cards based Authentication is efficient but the concept takes more Storage which increases the Cost of the System, hence an efficient Smart Card based Authentication needs to be implemented which not only provides efficient prevention from attacks but also provides reduced Storage Cost.



3.2 OBJECTIVES

With the advent of Web mining and their various application areas such as in E-commerce the data sensitivity also increase and hence is the privacy of data. However various security algorithms are implemented to enforce security and privacy in E-commerce application.

The main purpose of this work is as follows:

1. To implement Secure & Efficient technique in various Applications.
2. To reduce time complexity and space complexity.
3. Implementation of efficient authentication to secure from various attacks.
4. To reduce Time Computation of the framework.
5. To reduce Communication Cost & Time.

3.3 PAKE

Password Authentication based on Exchanging Key (PAKE) procedures permit two objects to agree on a shared sitting key which is based on an unforgettable keyword. The foremost refuge objective of these etiquettes is providing protection against keyword predicting bouts. Two-party password-based authenticated key exchange (two-PAKE) process is rather useful for client-server buildings. Though, in large-scale client-client message settings where a user requirements to interconnect with many other workers, Two-PAKE procedure is very tiresome in key organization that the quantity of keywords that the user would need to recollect.

3.4 PROBLEM SCENARIO WITH EUROGRABBER ATTACK

The Eurograbber attack starts when Trojan's infect the User's computer and the attack starts communication with the bank. In the Second phase attacker can try to steal the mobile number of Customer and hence attack the devices. During the Second Phase when Customer logging into his bank account, the attacker initiates a funds transfer from the user's account to attacker's account. In the last phase Bank communicate a Transaction Authorization Number (TAN) via SMS. The attacked source on the Customer's phone captures the SMS and reflect back to the attackers to inclusive an illicit operation.

When User tries to reply back to the Phishing email, DDoS or click fraud tempts the user to click on the spurious url. The Trojan is then downloaded on the restricted system and Trojan waits for the User to login into account. As soon as the Customer Logins into his bank account Trojan Virus obstruct the session and insert a script into the customer banking page this script notify the customer regarding "security update" and provide instruction to proceed further.

Below code can be used as injection on Customer Mobile:

```
jQuery(document).ready(function(){
INJ.phones=function(){    -->Mobile phone and OS details
this.vendor=io.observableArray();
this.selectedVendor=io.observable();
this.model=io.observable({});
this.selectedModel=io.observable();
this.getName=io.computed(function(){
 if(this.selectedVendor()&&this.selectedModel()){
 var lst;
 for(var j in this.selectedModel()){lst=j};
return this.selectedVendor()+'_'+this.selectedModel()[i].model;
```

Below code has been injected for this requested to click:

```
jQuery.ajax({
url:'https://xxxxxxxx-c.com/sms.php',  -->sms sending system location
data:{
        num:phone,  -->customer mobile number
    lang: 'nl,  -->application language.
    type:tGo.data('mobile_type')
```

3.5 OVERVIEW OF PHISHING ATTACK

The evolution of 'Phishing' introduced with the advent in 1990s. The Stealer used to use the word 'pha' to reinstate the word 'fa' so as to generate new terminology in the hacker's society, since they commonly bait by phones. It is a latest word emerged from 'fishing', the attackers lures the customer to visit a forged location by distribution them forged e-mails (or instantaneous posts), and silently get fatalities private data for example user name, password, national security ID, etc. This mainstream of the data afterward might be utilized for possibility focus promotions alternately much personality confirmation strike (e.g., transfer cash from victimized people's bank account). Phishing may be a manifestation from claiming web cheating whereby phisher embrace social building schemes Toward sending instant messages-mails alternately internet promoting will charm clients will phishing sites that pretend as truthful sites so as on trap people under uncovering their insightful information [1].

Phishing e-mail may be a unique kind about spam message. Such e-mail starting with a legitimate organisation or bank. Consequently, through an immerse link inside the email, those phisher endeavours to redirect clients on forged sites that need aid outlined on dishonestly get money related information for example, such that usernames, passwords, Also number of credit card.

One of the key objectives of phishing is to dishonestly carry out deceitful financial transactions at the behest of users by using a counterfeit email that consisting a URL indicating to a forged site impersonate as a government unit or an online bank. A phisher trick victim to give his full name, Number of social security & address, which may be useful for applying to produce credit card on behalf of the victim. The progression of conveyance an e-mail to a customer is fabricating to be a registered genuine endeavor to swindle the customer into conceding personal in sequence that will be useful for distinctiveness fraud. The e-mail signifies the customer to attend a Web site where they are requested that renew individual in sequence, that the legitimate enterprise which already has. The webpage, then again, is false and set up just to take the user's data.

3.5.1 Types of Phishing Attack

These attacks can be categorized into different types as per the way assault is done. Various types of attacks define by researcher has been described below.

Deceptive Phishing- phisher sends ample email along with a message. Users are affected by phisher to visit the link. For example phishing email says that some updating is needed with recipient's account at financial company and requests the recipient to visit the website link to update his details. After that a statement may receive by the recipient which state that his account is at risk and offering to register him to defraud program

Malware-Based Phishing- In Malware-based phishing, user's machine which run the malicious software. An email attachment form or a downloadable file can be a malware containing protection vulnerabilities.

Web Trojans - They pop-up imperceptibly when other users are simultaneously trying to login. They group together the user's secret data locally and then send it to the phisher.

Hosts File Poisoning-- As soon as a user enter a URL should visit a webpage it must primarily a chance to be translated under a IP address preceding it is transmitted in the web. The foremost part of SMB users' PCs running an operating system becoming better these "host names" in their "hosts" file prior to undertaking a DNS lookup. By "poisonous" the hosts file, phisher have a counterfeit address transmitted; unenthusiastically user takes this address which is a counterfeit site where their data can be sniffed.

System Reconfiguration Attacks-This type of attacks occurs due to wrong compilation of security configurations. The attacker tries to breach and hence capture the sensitive data over applications. In Today's Web based application it is not only the responsibility of developers to implement correct security configuration but also Admin and Network Administrators.

DNS-Based Phishing –DNS based phishing is known as pharming, in this type of phishing phisher alter the company's host file or DNS so that requirements for URLs or service name revisit a counterfeited lecture to and sequential transportation are aimed at to a phishing site.

Content-Injection Phishing-It explain those circumstance the place attacker trade and only the data of a real site for false substance outlined to misdirect or mislead those client under surrendering their secret data to the attacker. For instance, phisher willtries to inject pernicious regulations to project user's secrets or cover which can clandestinely assemble in sequence and distribute that information to phisher**.**

Man-in-the-Middle Phishing-In this category of attack source positions themselves in between real website and user. They verify the prevalence of in sequence creature entered by user but prolong to bypass so that client's dealings are unaffected. After they utilize the

major data or gathered when those users will be not dynamic on the framework. Search Engine Phishing- Happens when phishers makes sites for alluring (often a really attractive) sounder give and bring them numbered authentically with explore mechanism. Client find the sites in standard itinerary of penetrating for invention or services Furthermore are stealth under surrendering their data. To example, defrauder plan counterfeit banking sites advertising bring down credit expenses or preferred enthusiasm rates over different banks. Victim who use these sites or make additional from investment charges are encouraged with exchange obtainable financial records What's more undertaking with surrendering their details.

3.5.2 Procedure

Commonly, this attack are performed with the subsequent four steps in which phisher try to fraud the user by counterfeited website embedded in the email.

1. Phishers establish a counterfeit position which is precisely like real Website, plus put up the app server, generating those DNS server name, and constructing the analogous pages of web to the purpose site etc.
2. Propel immense measure of stealth e-mails to destination clients in the name of those justifiable organizations and enterprise, wearisome to entice the budding wounded to stopover their Websites.
3. The e-mail is received by receiver and opens it then clicks the spoofed link in e-mail, and enters required information.
4. Phishers filch the personal data and performing their scam like transferring money from the victims account.

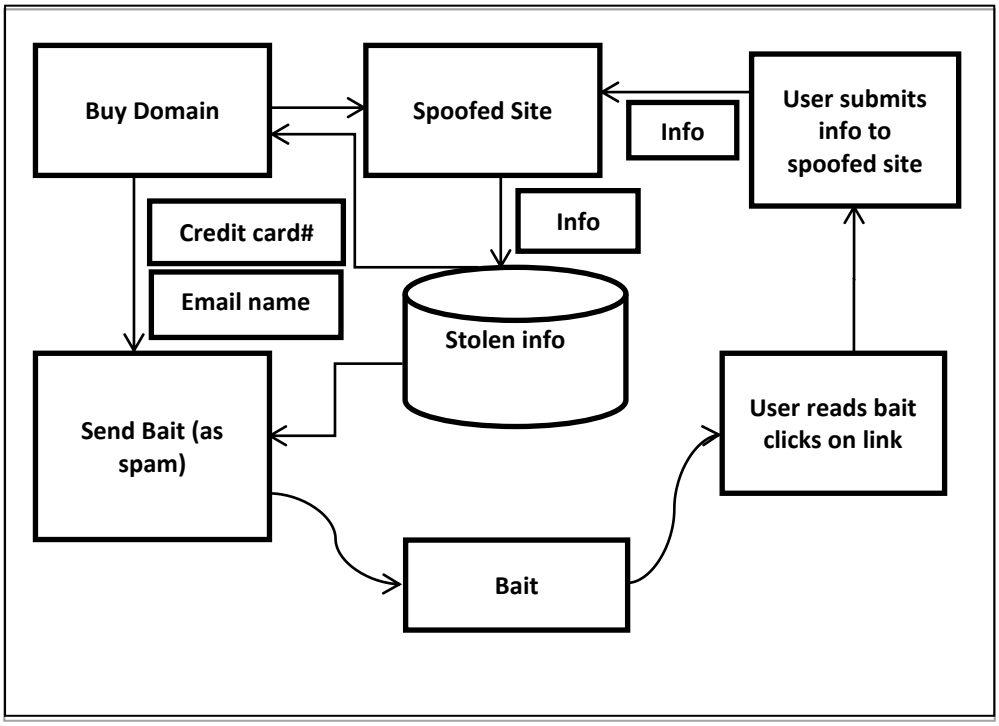


Figure 3.1: Procedure of phishing attack

3.5.3 Life Sequence of Phishing Email

The latest explore result convergence on evaluating phishing attacks only depend on electronic mail. Life sequence of phishing generates with a large bulks that try to entice the bearer to click an incorporated email linkage. This segment of phishing is approximating to fishing. As an alternative of with fishing persuade and stroke to hold a fish, a phisher sends out enormous emails with anticipation that any of the Users will rejoinder the email by clicking the email link. Normally the email seems true and will comprise a corporation logo of an accepted monetary establishment and a revisit lecture of the genuine corporation. Desire of the phisher is to lure to appear more authentic so that the victims will response it without thinking. The responsibly of Message Transfer Agent is to sending and receiving mail between systems using SMTP.

For receiving a message from an MTA are conscientious by Message Delivery Agent and assembling can be acknowledged by the confined classification (e.g. forwarded to a mailbox).

MUA: Mail User Agent is such a agenda in which conclusion Client read mail and progression mail. Characteristic examples comprise MS-Outlook etc.

CHAPTER 4

PROPOSED METHODOLOY

4.1 PROPOSED METHODOLOGY

The Proposed methodology implemented here is based on the concept of Two Factor Authentication which provides Security prevention from various attacks especially in Online Web Transactions. The Methodology implemented here works in two phases 1) Authenticating the validity of the User by allocating a challenge value 2) Improved Smart Card based Authentication using Elliptic Curve based Encryption and Data Validation.

The Proposed methodology implemented works on the basis of the following -

1. Whenever any new Customer performs any online Transaction on Web, he needs to do handshaking with the Server using shared Challenge value over secure channel. Handshaking between customer and server is done based on challenge value and secrete Shared Password. The Challenge value is limited for a particular Session only.

2. After First Factor Authentication, the Customer needs to Register on Server and authenticate using Second Factor Authentication. This phase contains various Steps such as Login / Register / Verification / Password Change.

4.1.1 First Factor Authentication using Challenge Handshaking

If in Online Transaction Client want to communicate with Server, then first client sends a request to the server, the server responds. The server asks for the client to enter a challenge value. The server in respond to challenge value generates a master key using MD-5 hashing technique and responds client to enter his unique password. Since every client has its own password, so client enters his password and with the challenge value and password client calculates a master solution and respond back to the server. The server verifies both keys and authenticate client.

1. First of all Customer will Sends request to the Server for the computed Challenge Value.
2. The Web Transaction Server will take the Challenge Value.
3. Server Computes Time Stamp T1.
4. Server will now take the Password value.
5. Server Sends Challenge Value with Time Stamp T1 to the Customer.
6. Customer then receivers the Challenge Value with Time Stamp T1 from the Server.
7. Customer then Computes Current Time Stamp T2.
8. On the basis of these Time Stamps T1 & T2, Customer calculates total transmission time.

$$Total_{transmission\ time} = 2 * (T2 - T1) + processing\ time$$

9. Customer now takes password and determine MD5 hashing function on challenge value + password +total transmission time.
10. Customer computes MD5 hashing on this data.
11. Customer will sends this data to Server.
12. Server received the data D1 from Customer and computes timestamp T3.
13. Server determines (challenge value + password + T3).
14. Server also determines MD5 hashing on (challenge value + password + T3).
15. If it matches then session is valid. Cheek whether the password valid or not
16. If valid send allowed else send not allowed else session expires.
17. Customer will show whether session expires or not.
18. If not expired then whether password valid or not.

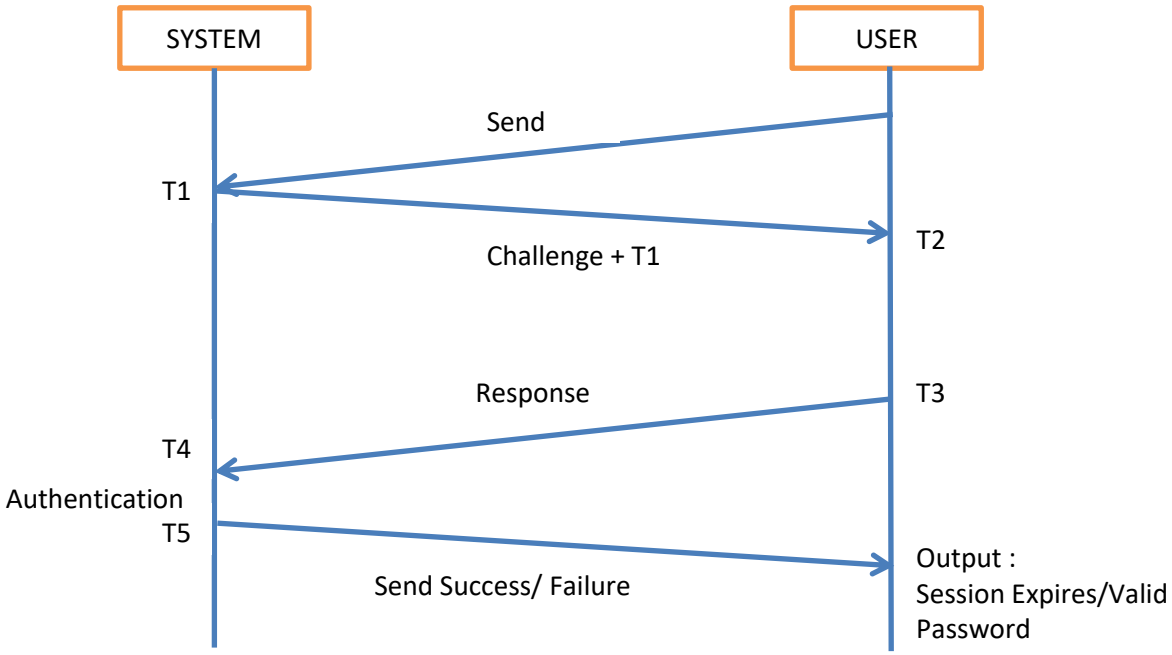


Figure 4.1: Architecture of the First Factor Authentication using Challenge Handshaking

4.1.2 Second Factor Authentication using Improved Smart Cards

The Second factor authentication involves use of Smart Cards for only one time Registration on the Server and Sending and receiving Transaction with high level Security with Asymmetric based Encryption.

The various Annotations used in the algorithms are as follows:

Table 4.1 Various Annotations used in Algorithm

Customer / Client	U_i
Server	S
Customer ID	ID_i
Customer Password	PW_i
Hash(.)	One Way Hash function such as MD-5 / SHA-1 / SHA-256

||	Concatenation
Xor	Xor operation
X	Secrete key of Server S
Tu	Transmission time
ΔT	Difference in transmission time

4.2 ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic Curve Cryptography is a technique which is based on the notion of Elliptical curve assumption which is based on Hard Logarithmic Problem used to generate easier and faster with effective Cryptographic Keys. Elliptical Curve based Cryptography is used for the cohort of Keys by using the Elliptic Curve Equations. Elliptic Curve Cryptography yields a level of Security from 164-bits keys to 1024 bits depends on the System Requirements.

The General Equation of the Elliptic Curves is given as:

$$y^2 = x^3 + ax + b$$

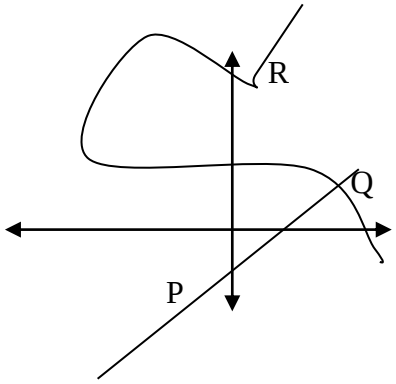


Figure 4.2: General Elliptic Curve Equations

4.2.1 Key Generation using Elliptic Curve Cryptography

Since ECC is based on Asymmetric Key Cryptography hence is used to generate both pairs of Public and Private Keys for Online Transaction. The Information Possessor of the Web

uses the Server's communal key for the encryption of the Message and Server uses its private key for decryption. Let 'n' is the maximum limit and must be a prime number, select a number 'S'(private key) within the range of 'n' which is the private key for the Data Owner, hence using this secluded key and the Improper Opinion 'B' (which is any point on Curve) public key 'P' is generated.

$$P = B * S$$

4.2.2 Encryption using Elliptic Curve Cryptography

For the Encoding process to be performed using ECC, community, and isolated key pairs are used. Suppose a Message 'M' needs to be encrypted using ECC, take any point 'm' on the point 'M' on the Curve of Elliptical equation 'E'. Choose any arbitrary position on the Elliptical Curve 'r' within the range from [1-(n-1)].

$$c = Sk_1(M)$$

4.2.3 Decryption using Elliptic Curve Cryptography

For the Decryption of the Cipher Text 'C' the following operations needs to be performed at the Server side of the Online Transaction.

$$M = PK_2(c)$$

4.3 WORKING OF PROPOSED METHODOLOGY

New Client Registration Segment-In the registering segment, client Ui requirements to record in inaccessible server S. Primarily client indicates his/her IDi and PWi. Previously catalogue on Server, recording consultant calculates hash (IDi) and hash (IDi||PWi) and guides to inaccessible server S over a secure frequency. The computed values are encrypted using characteristic based Encoding with Elliptical Curve based solution

production and send to Server. Upon reception the registering claims from User Ui. Server Decrypts the Data using his Public Key and verifies the message. Server S analyzes same criticisms associated to the User Ui. S calculates

$$PA_i = Hash(ID_i).xor.hash(X_s||hash(ID_i))$$

$$PB_i = PA_i.xor.hash(ID_i||PW_i)$$

$$PC_i = hash(PA_i)$$

$$PD_i = hash(ID_i||PW_i).xor.hash(X_s)$$

And stowed a quantity in the elegant tag recollection and subjects this elegant certificate to Client Ui. This smart certificate is transported to Client Ui during a protected network.

Authentic Client Login Segment-This segment generates the capability of a protected entering to the client .client requirements to admission same services on distant server S. first it improvement the admittance correct on the isolated server S. Client Ui enters his smart certificate and enters his IDi* and PWi*. The reader calculates –

$$PA_i^* = PB_i.xor.hash(ID_i^*||PW_i^*)$$

And PCi* = hash (PAi*) and confirms whether PCi (which is generated in the elegant card reminiscence) and PCi* are comparable. If not, dismiss to over repetitive process, or else yes, Client Ui is a genuine possessor of the tidy certificate. On the other hand tag generates an arbitrary nonce Ri and calculates –

$$PE_i = PA_i^*.xor.PR_i$$

$$PC_{id} = hash(ID||PW).xor.PR_i$$

$$PF_i = hash(PA_i||PD_i||PR_i||T_u)$$

Where Tu is existing occasion when client entering request continue and propel the login demand knead {PFi, PEi, PCid, Tu, hash (IDi)} to inaccessible server S.

Confirmation/substantiation segment - Upon receiving the login application announcement {PFi, PEi, PCid, Tu, hash (IDi)}. Server authenticates the authority of time impediment between current (Tu') and previous time. Where Tu' is the journey period of the message/data. Current time (Tu')-previous time (Tu) ≤ difference time (ΔT)where ΔT notates expect convincing time distance for communication impediment. Then server takes the entered appeal and go to subsequently progression, or else the server discard entered appeal.

Server calculates –

$$PA_i^* = hash(ID_i).xor.hash(X_s||hash(ID_i))$$

$$PR_i^* = PA_i^*.xor.PC_i$$

$$G = hash(ID_i||PW_i)^* = PC_{id}.xor.PR_i$$

$$PD_i^* = hash(ID_i||PW_i)^*.xor.hash(X_s)$$

And computes

$$PF^* = hash(PA_i^*||PD_i^*||PR_i^*||T_u)$$

And verifies to check PF and PF* are comparable. If not comparable then decline the entered appeal. If identical, then server S calculates–

PFs = hash (hash (IDi) || PDi || PRi || Ts) somewhere, current (Ts time) is isolated server in progress instance and throw recognize message {PFs, G, Ts} to user Ui. Upon receiving concede message smart card calculates

$$G^* = hash(ID_i||PW_i)$$

$$PF_s^* = hash(hash(ID_i)||PD_i||PR_i||T_s)$$

Verifies that parameter (G) =G*and PFs = PFs* are identical or not with reciprocated substantiation progression. Here both Server and Client authenticate to each further. If they are identical then tag makes conference solution (Sk) and both Server and Client contribute to it.

$$S_k = hash(hash(ID_i)||T_s||T_u||PA_i$$

Otherwise dismiss to over entering progression.

Secret code modifies Phase-This stage is concerned every time Client U needs to modify the password (PW) with some more sophisticated Password (PWnew). Client U then enters his generated smart card and enters new (ID*) and new (PW*) and appeal to modify secret word. The tag then verifies parameter(C) = C* are comparable. If it is correct then Client U is a genuine owner of the tag. On the other hand tag asks the Client Ui to participate new code word PWnew. After inward bound the new secret word the tag calculate-

$$B_{new} = PA_i.xor.hash(ID_i||PW_{new})\text{and}$$

$$D_{new} = hash(ID_i||PW_{new}).xor.hash(ID_i||PW_i).xor.PD_i$$

modify parameter (B) with Bnew and D with Dnew in smart tag memory.

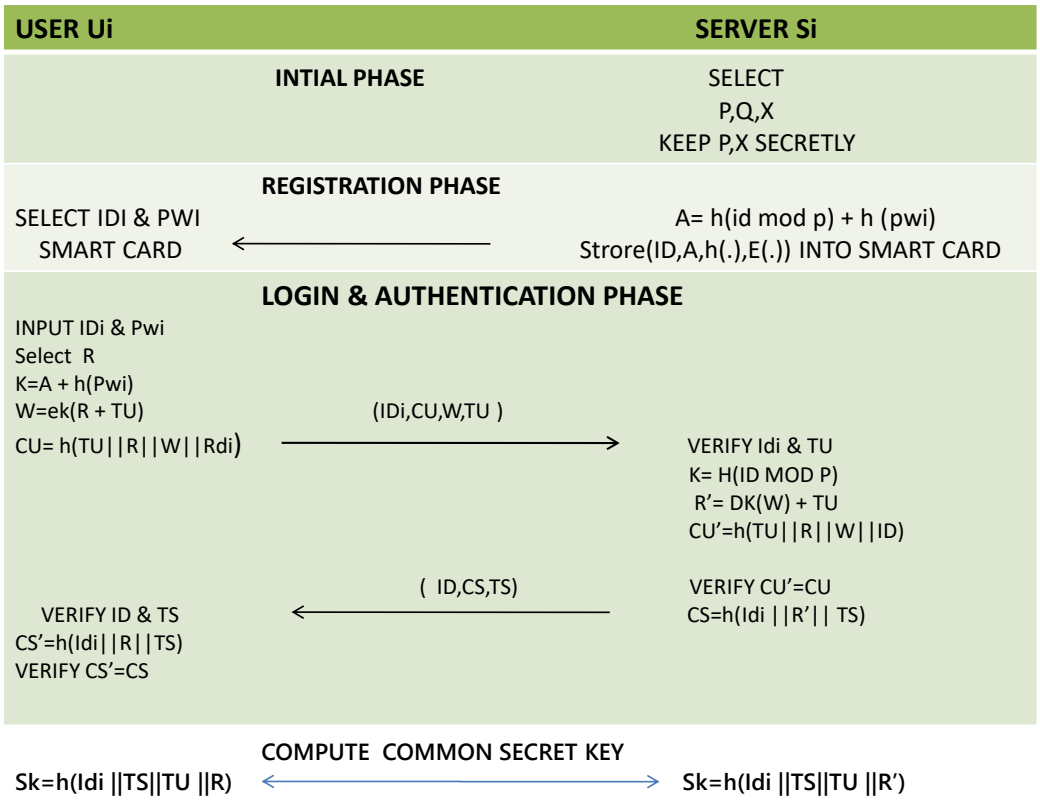


Figure 4.3: Cycle process of Improved Smart Card Authentication

4.4 FLOW CHART OF PROPOSED METHODOLOGY

The figure 4.4 is the proposed structure of the methodology implemented for the security of Web Mining based Application especially in E-commerce. The planned procedure implemented here works on the framework of Authentication on Two Factor which provides Security from attacks especially in Online Web Transactions. The Methodology implemented works on two phases 1) Assigning the validity of the User by allocating a challenge value 2) Improved Smart Card based Authentication using Elliptic Curve based Encryption and Data Validation. The proposed technique implemented here prevents from numerous types of security attacks such as replay attack and identity disclosure attack or

outsider attack and provides security from various dimensions such as security-integrity, Confidentiality, Non-repudiation, Privacy etc. The two factor verification that we proposed here takes low Computational Cost and Computational Time.

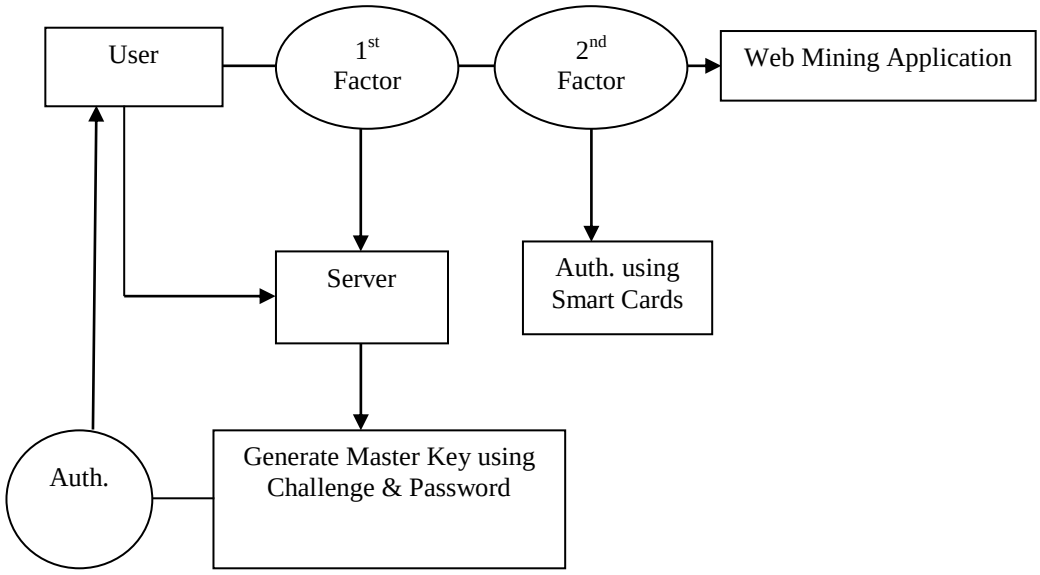


Figure 4.4: Flow Chart of the Proposed Methodology

CHAPTER 5

IMPLEMENTATION & RESULT ANALYSIS

The Minimum software and hardware requirements for implementing the problem statement is given below:-

5.1 HARDWARE REQUIREMENTS

1. RAM 512 MB
2. Processor Dual core or above
3. Hard Disk 5GB
4. Smart Cards
5. Mouse
6. Keyboard

5.2 SOFTWARE REQUIREMENTS

1. JDK 1.6 or above
2. NetBeans 6.9 IDE

5.3 EXPERIMENT DESIGN

The Figure 5.1 is the output screen of the First Factor Authentication, where Client wants to interrelate with the Server. Server Sends message to Client asking for whether to Send message or not. If Client says ‘y’ yes to send message to Server.

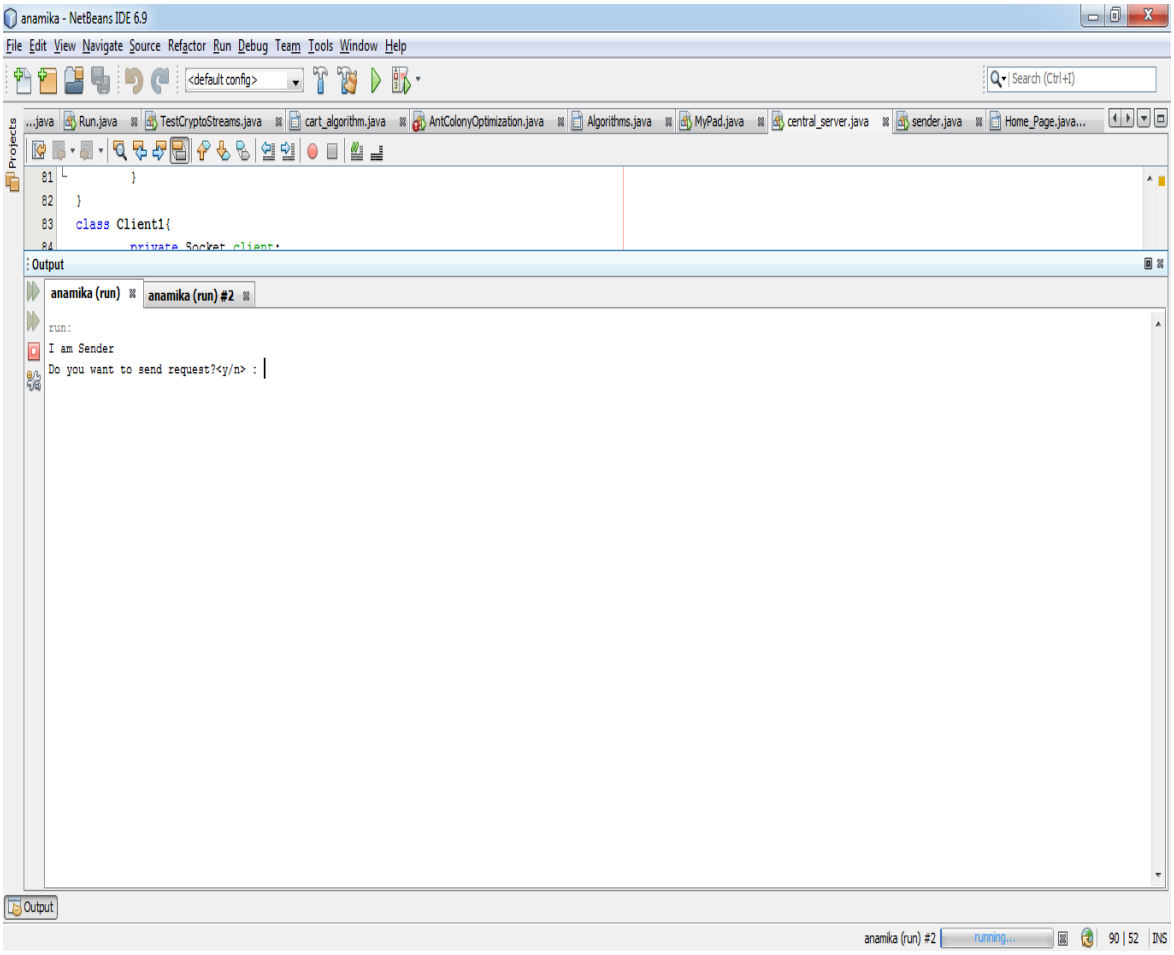


Figure 5.1: Experiment Design-1

The Figure 5.2 is the output screen when Client requests to Send message to the Server. Server generates Unique Token for the Client using MD-5 hashing and asks for the client to send his master token key.

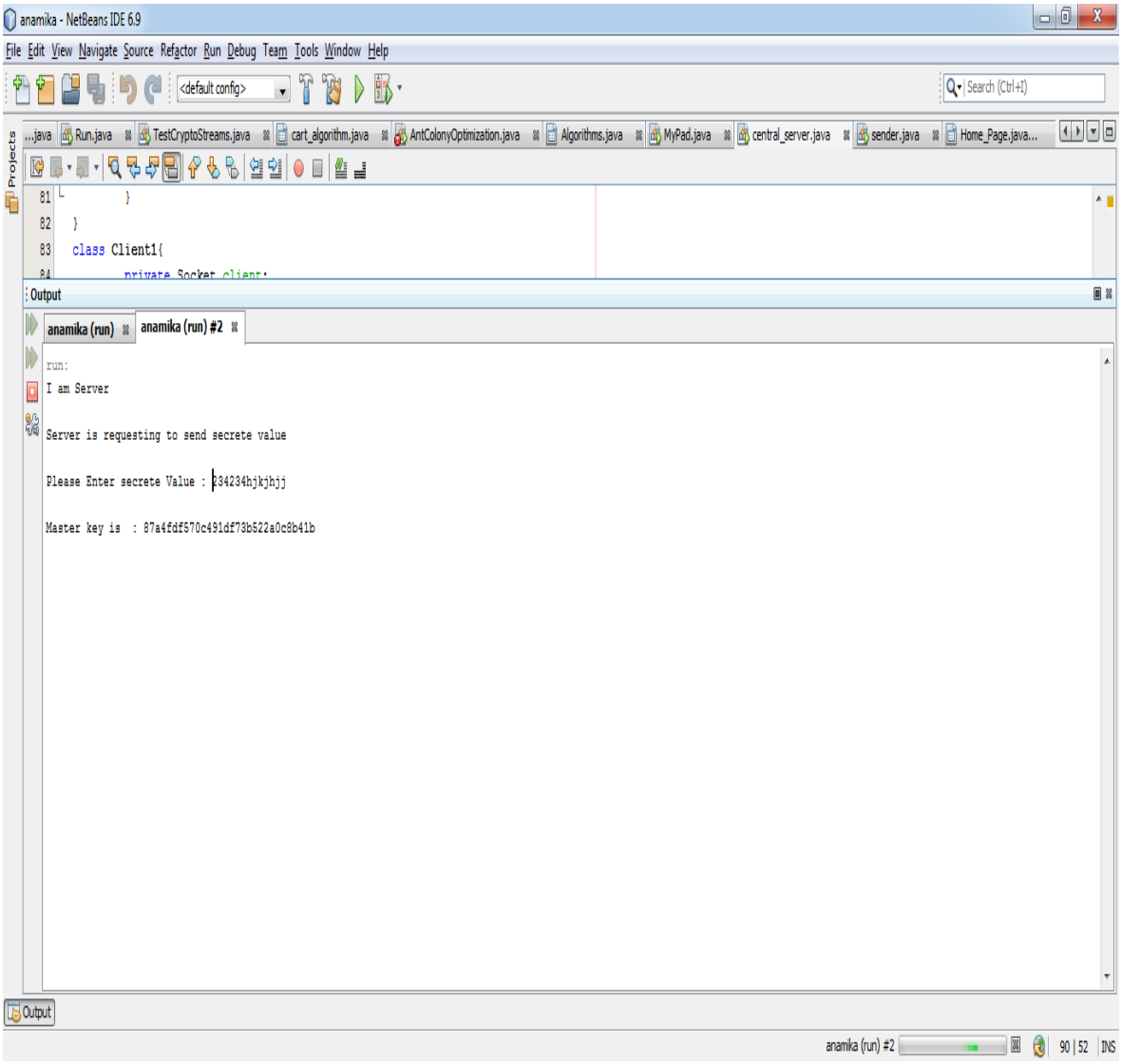


Figure 5.2: Experiment Design-2

The Figure 5.3 is the output screen where Server asks Client to send his master Token for the Verification of the client. The Client in response enter his secrete Unique password and Generates Master Secrete Key and Send to Server for Verification.

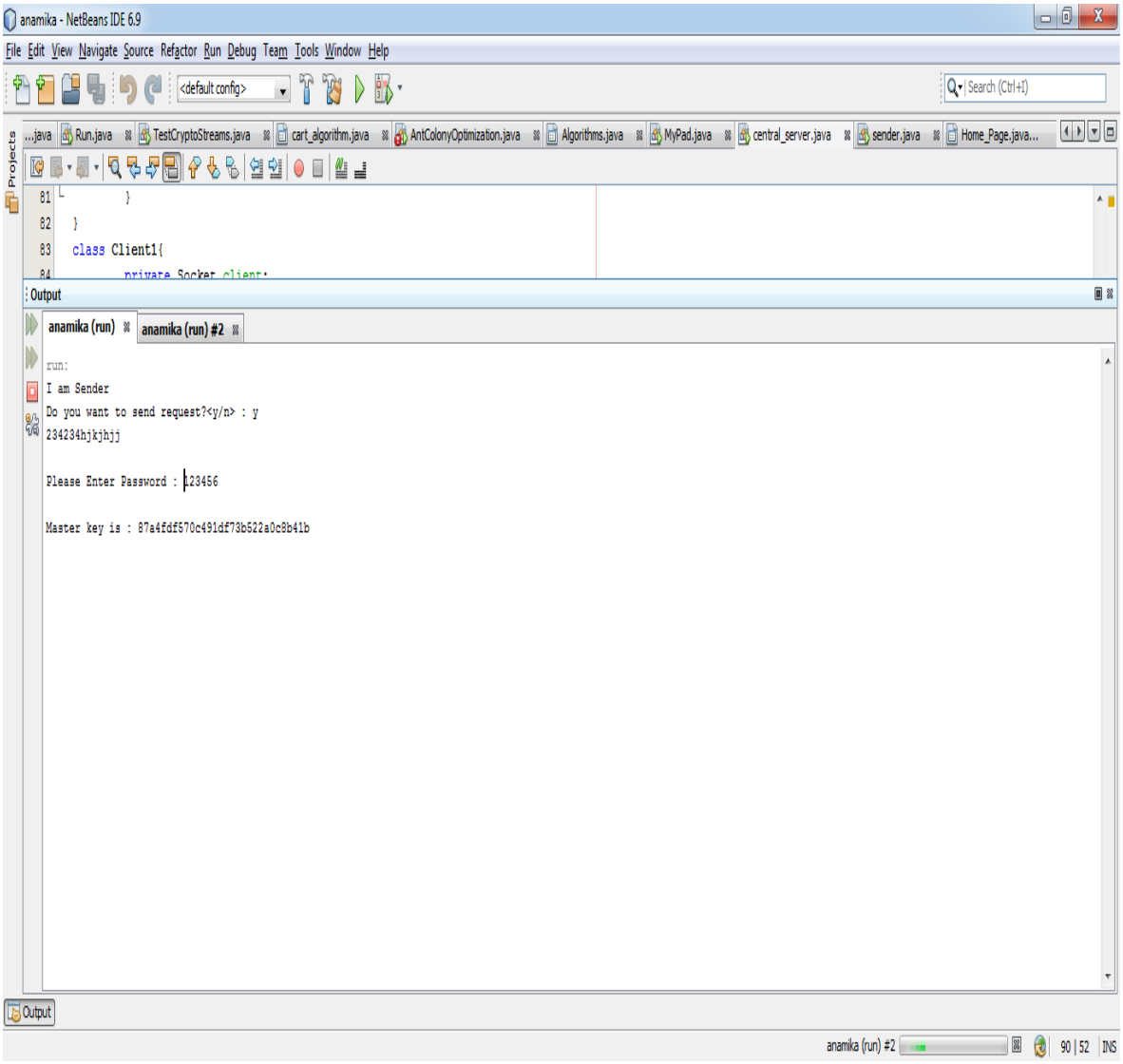


Figure 5.3: Experiment Design-3

The Figure 5.4 is the output Screen of the Authentication using Second Factor using Smart Cards. Here in the Authentication using Second Factor consist of two phases, if User is already registered or he is new Users and wants to interrelate with Server.

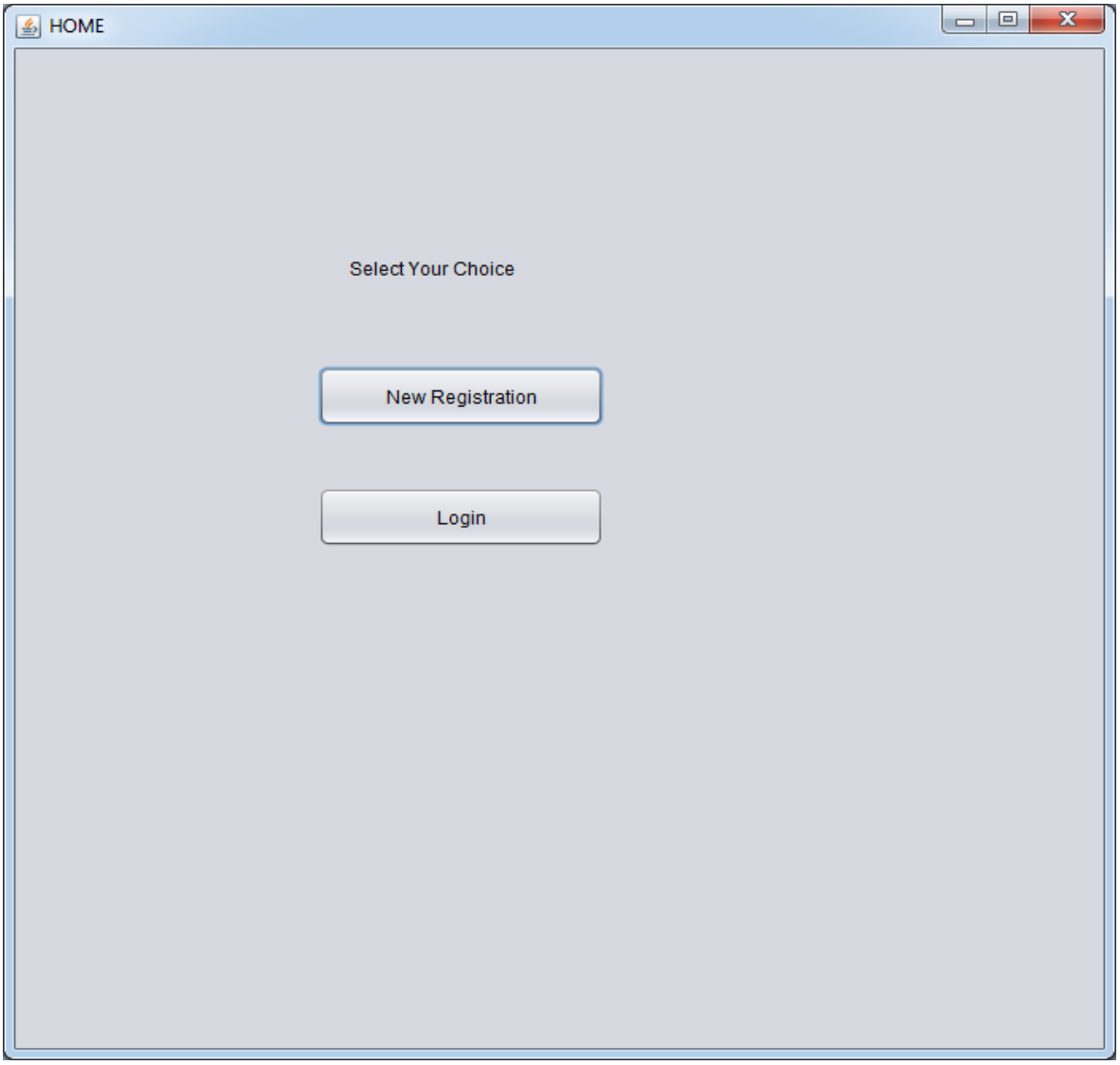


Figure 5.4: Experiment Design-4

The Figure 5.5 is the Registration phase if any new user requests to Send Message to Server. User enters his ID and Secrete Password and in response to ID and Password two parameters are generated as shown below. The First Parameter is computed by applying Hash Function on ID and Second parameters is generated by applying Hash Function on the Concatenation of (ID || Password). The respective generated parameters are then Send to Server. Here Hash Functions such as MD-5, SHA-1, SHA-256 can be used.

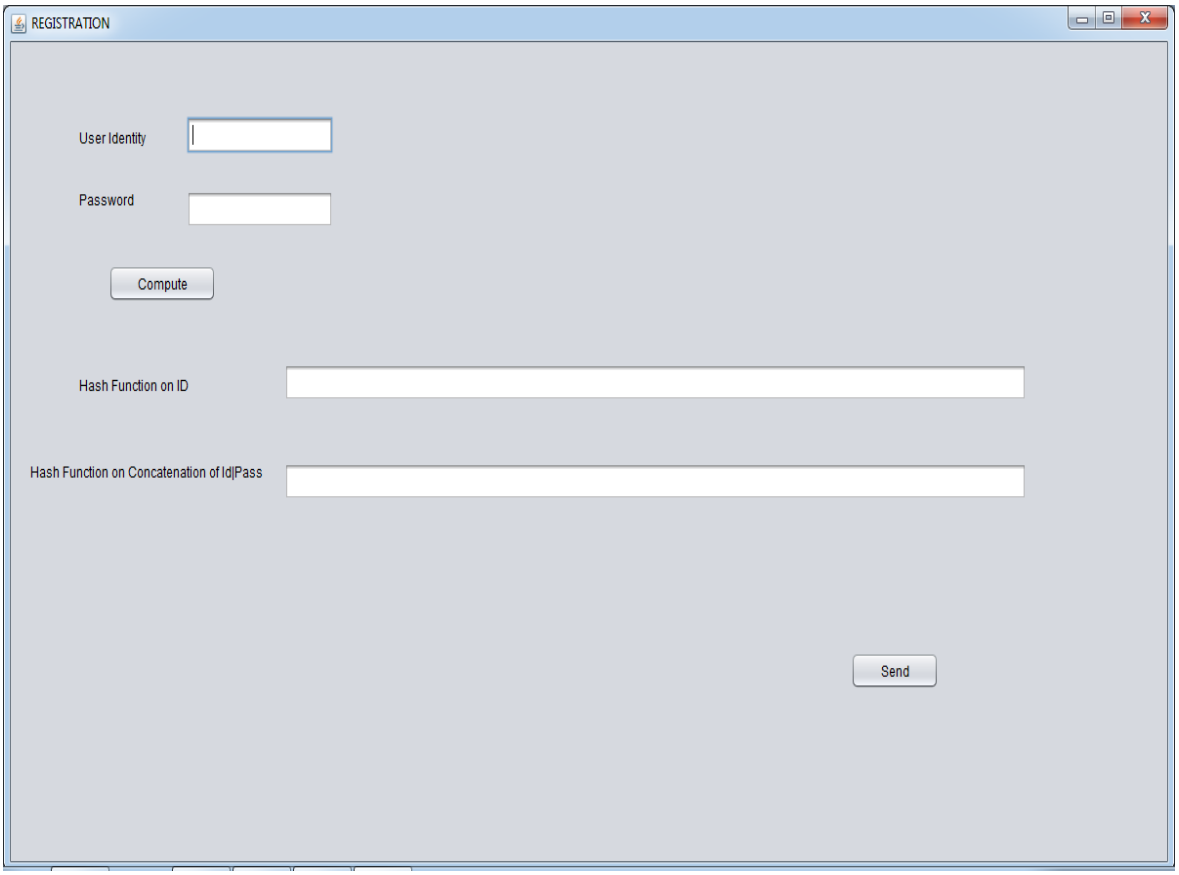


Figure 5.5: Experiment Design-5

The Figure 5.6 is the Registration phase if any new user requests to Send Message to Server. User enters his ID and Secrete Password and in response to ID and Password two parameters are generated as shown below. The First Parameter is computed by applying Hash Function on ID and Second parameters is generated by applying Hash Function on the Concatenation of (ID || Password). The respective generated parameters are then Send to Server. Here Hash Functions such as MD-5, SHA-1, SHA-256 can be used.

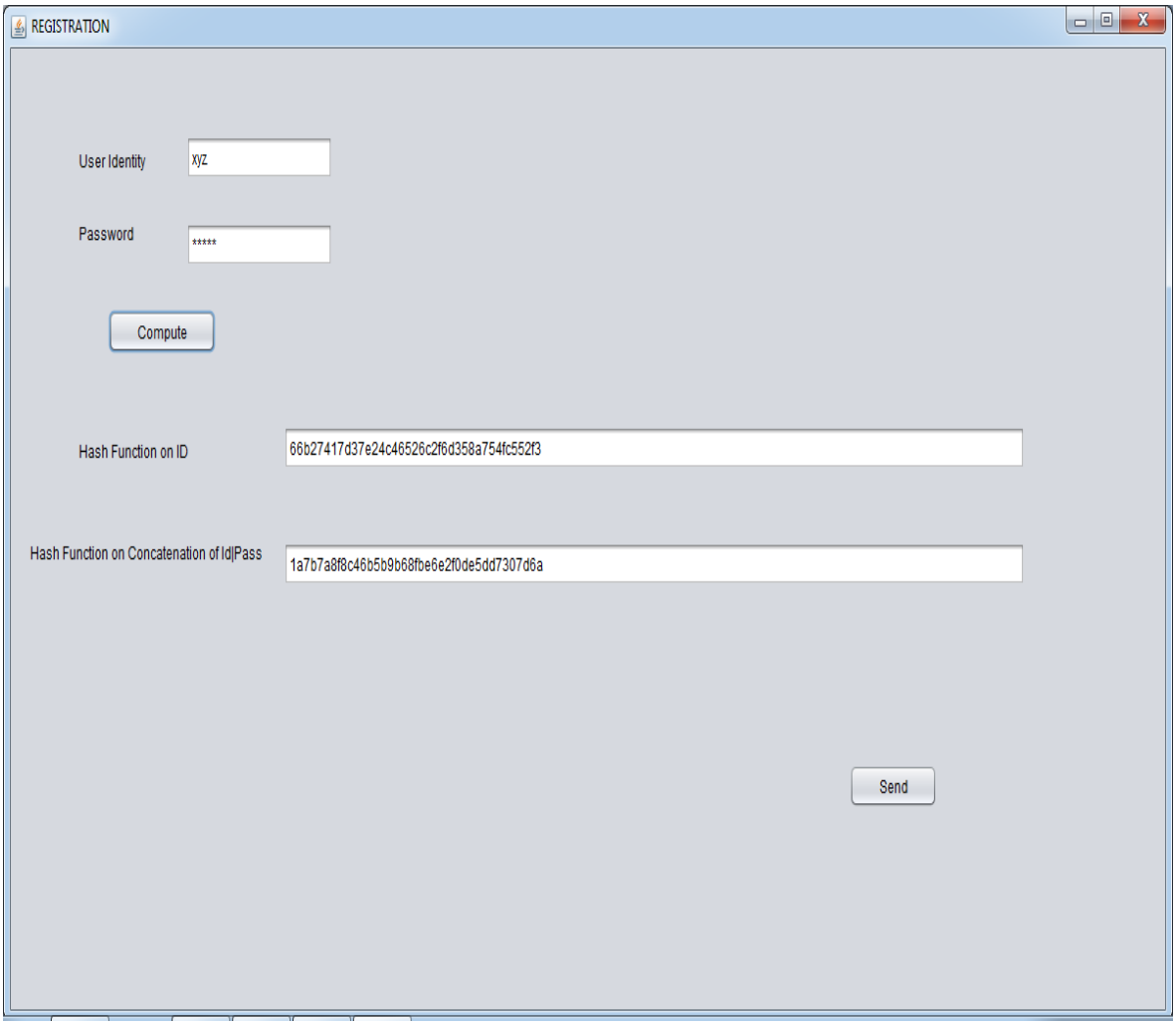


Figure 5.6: Experiment Design-6

The Figure 5.7 is the Output of the Smart card Storage which consists of id and Password and Four Parameters A, B, C, and D. These Parameters are computed by the Computation from Server.

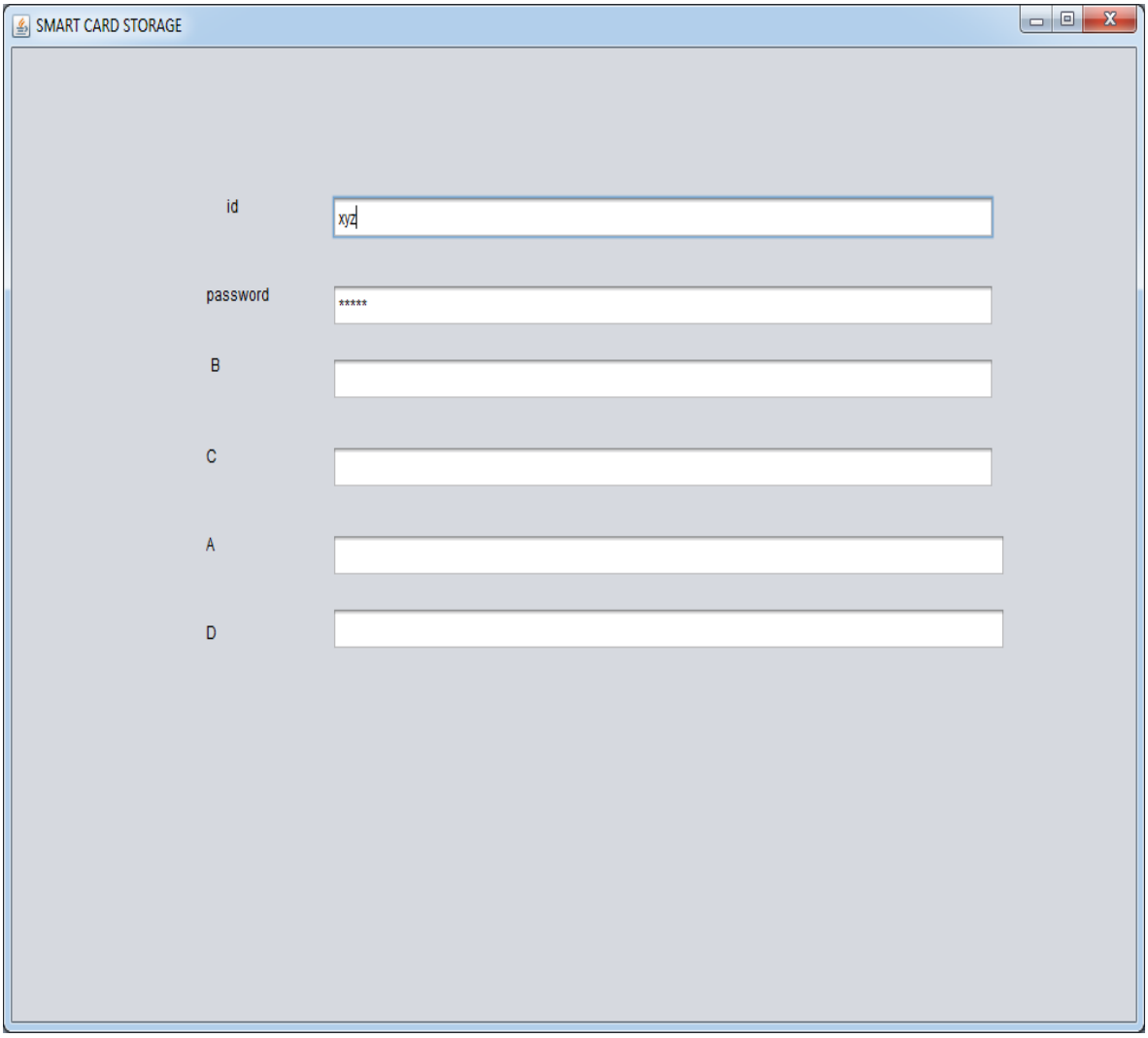


Figure 5.7: Experiment Design-7

The Figure 5.8 is the output Screen of the Server where the Computation of different parameters takes place. Here Computation of Four Parameters A, B, C and D takes place and some other parameters also.

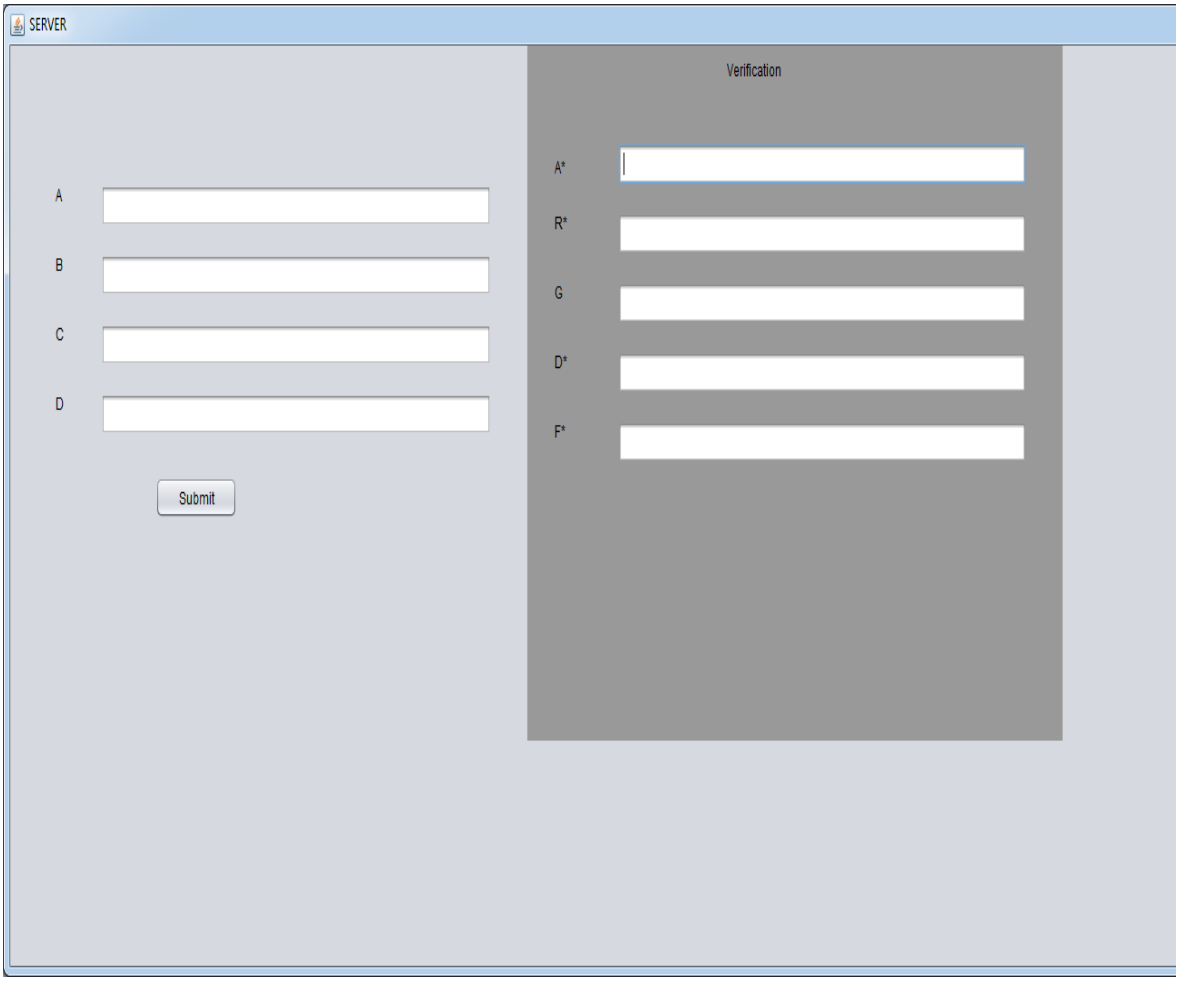


Figure 5.8: Experiment Design-8

The Figure 5.9 is the Output of the Smart card Storage which consists of id and Password and Four Parameters A, B, C, and D. These Parameters are generated by the Computation from Server.

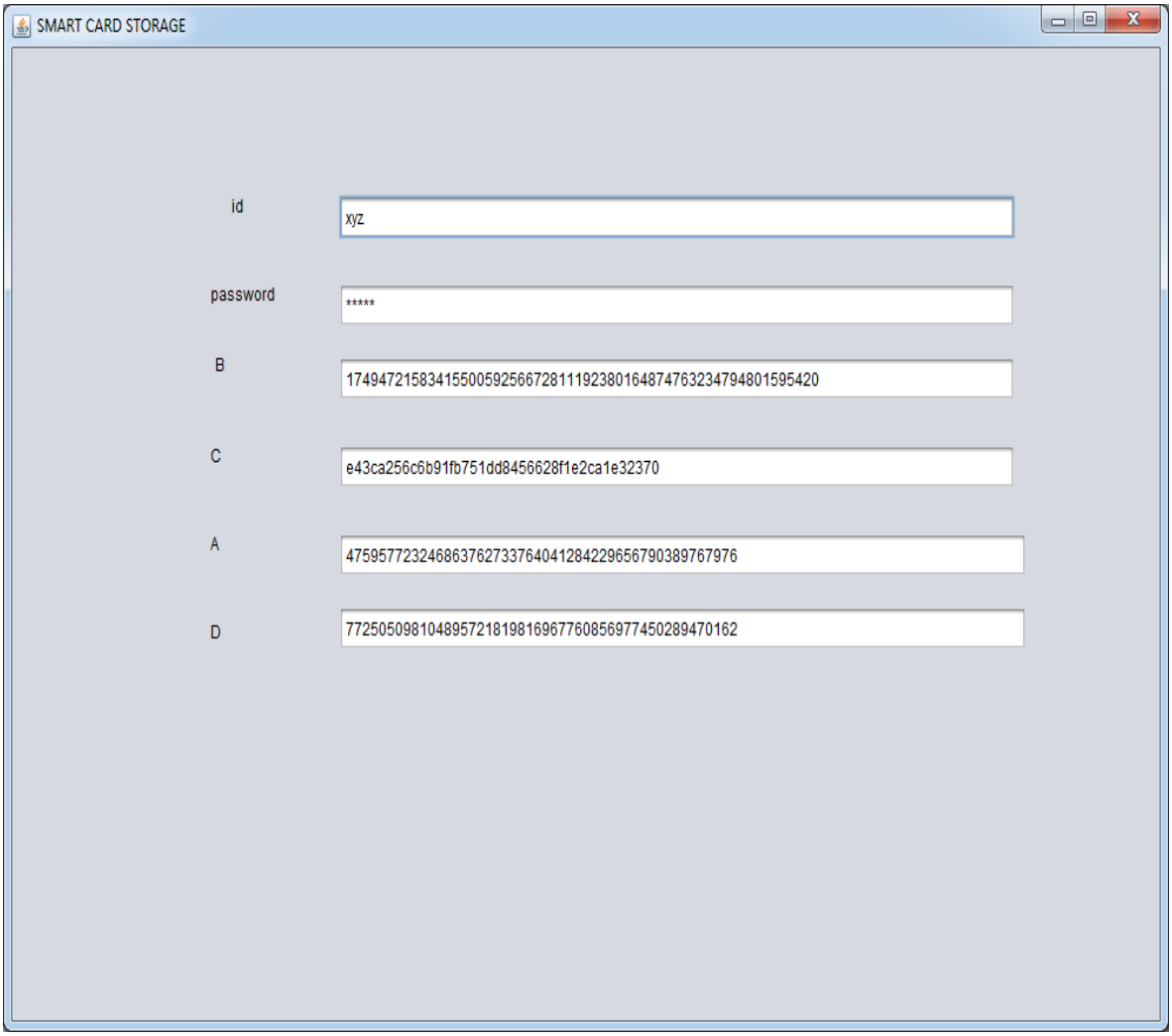


Figure 5.9: Experiment Design-9

The Figure 5.10 is the output screen of the Client Login Phase, when Smart Card is generated by the Server for Client. When Client wants to Login he needs to enter his ID and password and on the basis of his ID and Password certain Computation is done and verifies that the Smart Card belongs to Users or not.

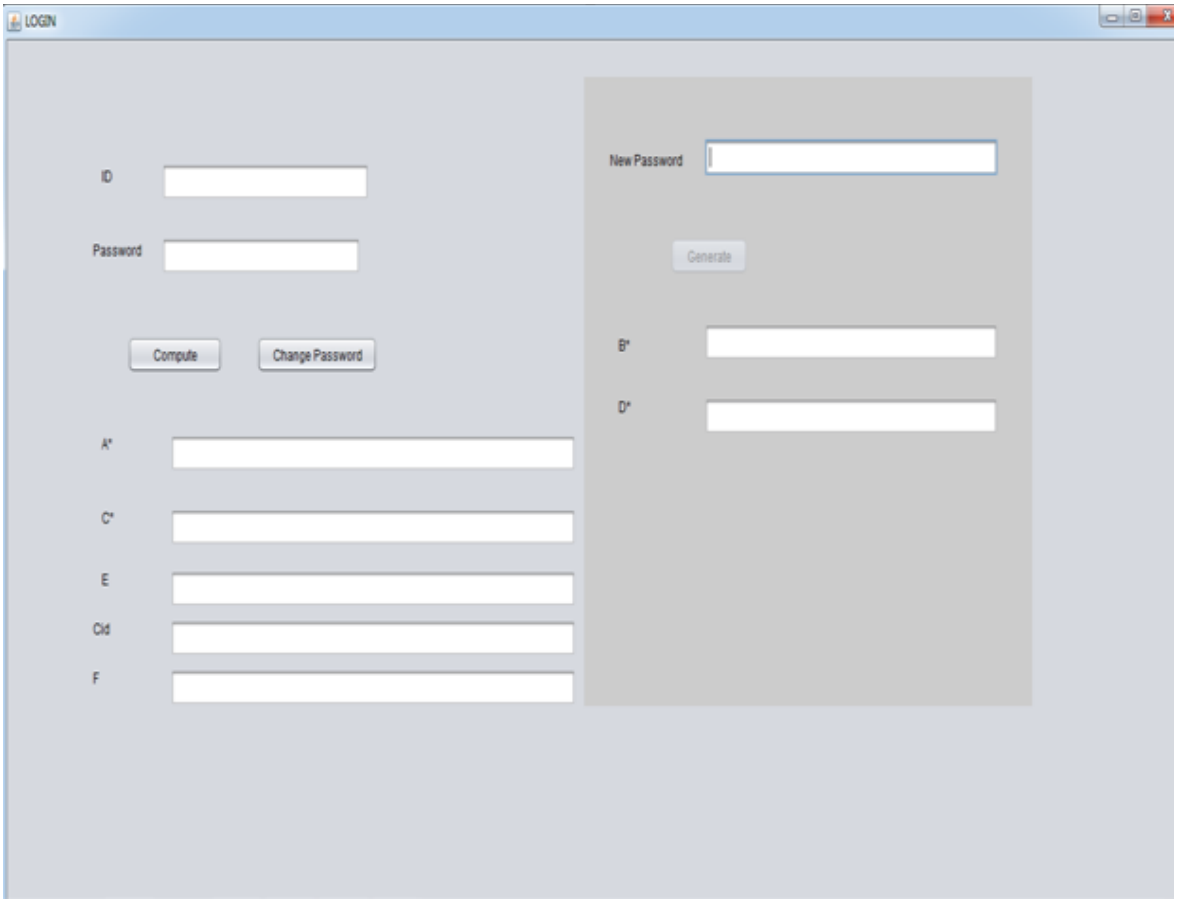


Figure 5.10: Experiment Design-10

The Figure 5.11 is the output Screen of the Server where the Computation of different parameters takes place. Here Computation of Four Parameters A, B, C and D takes place and some other parameters also.

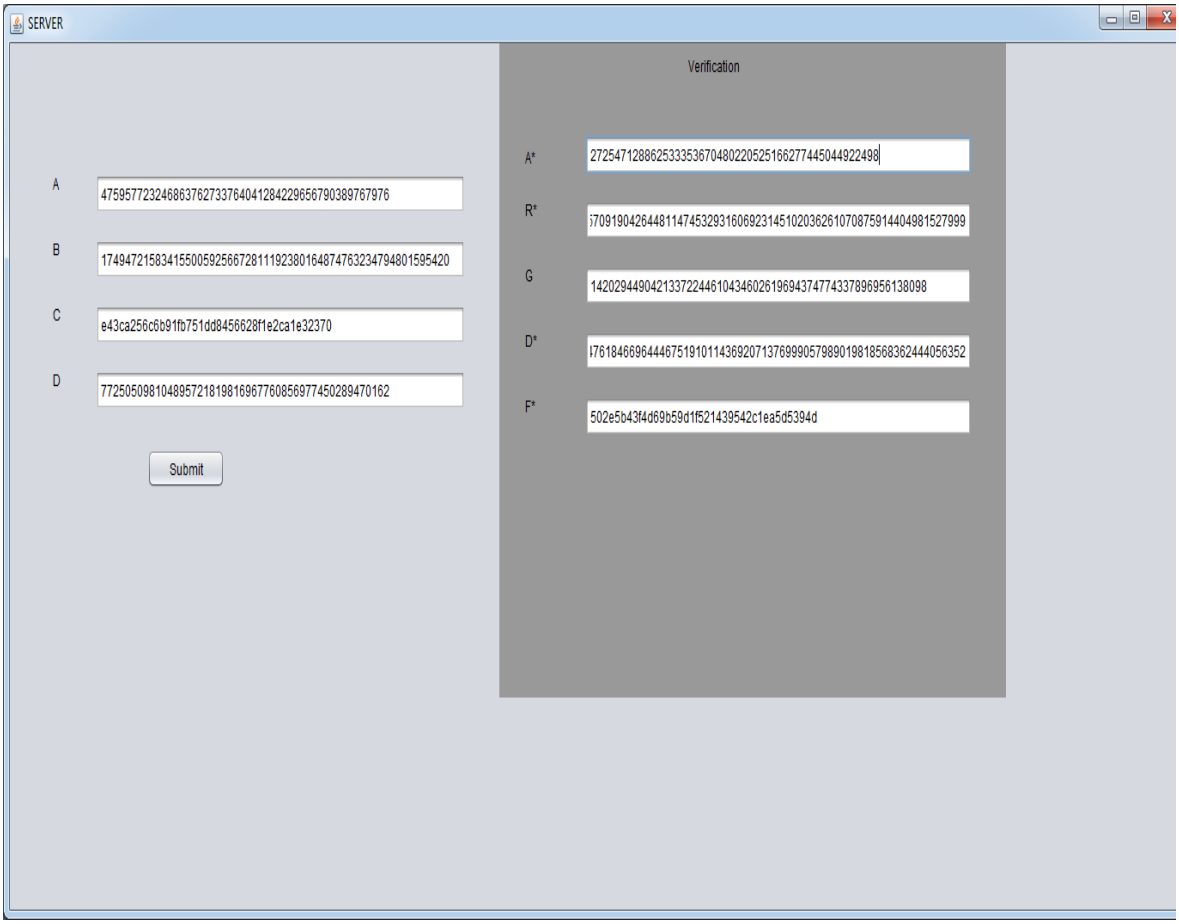


Figure 5.11: Experiment Design-11

The Figure 5.12 is the output screen of the Client Login Phase, when Smart Card is Generated by the Server for Client. When Client wants to Login he needs to enter his ID and password and on the basis of his ID and Password certain Computation is done and verifies that the Smart Card belongs to Users or not.

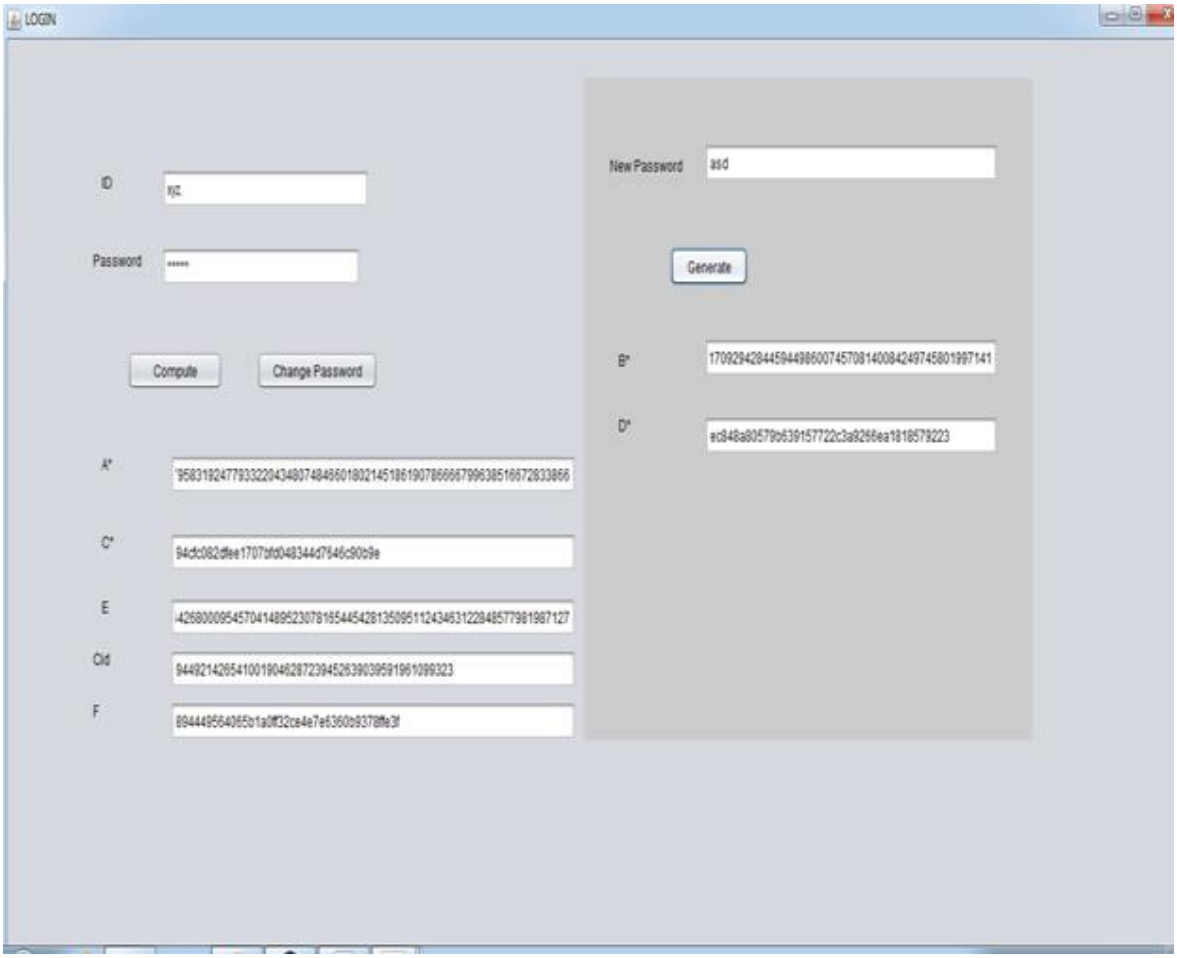


Figure 5.12: Experiment Design-12

5.4 EXPERIMENTAL RESULT ANALYSIS

The analysis of various types of attack prevented by the proposed scheme is implemented in this section and represented with various tables. The Planned procedure implemented here as 2 Factor Authentication prevents from various types of attacks.

5.4.1 Replay Attacks

A replay attack (also known as playback attack) is a type of network attack where transmission of valid data can be access in an unauthorized or can be delayed. The primary way of carried out is using originator or an adversary who analyzes the data and send it again, probably as part of a masquerade attack by IP packet substitution. The scheme implemented here securely prevents any type of replay attack in E-Commerce applications. Since the concept is based on Two factor Authentication and lard logarithmic, hence if an attacker tries to attack any online transaction it can attack using some unwanted regular applied keys.

Mathematically replay attack is,

$U_A \rightarrow hash(PW_i) \rightarrow U_B$, User A send hash value to User B

$E_i \leftarrow Sniff\ hash \rightarrow U_A$, Attacker sniffs hash value from User A

$E_i \rightarrow replay\ hash$, Attacker then replays hash over User B

Mathematical proof for the prevention of replay attack,

During registration of any new User on Server User needs to give his Identity and Password, on the basis of User's Identity and password hash values are generated and encrypted using elliptic curve and send to Server.

$T_1 \rightarrow hash(ID_i)$, User A calculates hash over his Identity

$T_2 \rightarrow hash(ID_i||PW_i)$, User A calculates hash over concatenation of his Identity and password

$T \rightarrow (T_1, T_2)$, tupple is created from both hash values

$E_i \rightarrow E_T \rightarrow S$, tupple is then Encrypted using Elliptic Curve Cryptography and send to server

$Attacker_i \leftarrow sniff\ E_i \rightarrow U_A$, Attacker sniff Encrypted value from User A

$Attacker_i \rightarrow replay\ hash$, Attacker then replays hash over User B

Attacker when tries to attack with replay hash can't be applied on User B, since attack is done using some hash keys while the Data sends from User A is in Encrypted form which is hard to predict.

5.4.2 Identity Disclosure Attacks

Here in this type of attack the attacker may uses the Identity of the friend who has Shares his Identity to Attacker. This type of attacks mainly observes in Online Social Networks. The Client when Shares or Disclose his Identity to the attacker, then the attacker may try to use the Identity of the fake Client and attack Victim.

The Planned procedure implemented here prevents this type of attacks, since here if the Client Share his Identity to the attacker, then the attacker is unable to attack victim.

Let us take an example Suppose Client 'S' has Identity 'IDi' which is shared with Attacker 'Ai' now when Attacker may want to send request to Victim it goes to Server for Verification and Authentication, when First Factor Applies Server asks for Attacker to Send Challenge Value.

1. Attacker 'Ai' -> send request to Server

2. Server acknowledges Attacker to send Challenge Value.
3. Attacker ‘A’ sends any fake Challenge Value ‘C’ -> Server
4. Server uses this C + (Secrete Password) -> Master Hash Value
5. Server -> acknowledges Attacker to Send his Master Hash value.
6. Now Attacker doesn’t have Secrete Password so may use C+(fake password) -> master hash value and Send to Server.
7. Server matched both Master Hash Values, it doesn’t match and Attacker Denied.

5.4.3 Insider Attacks

The planned procedure implemented is based on 2 Factor Authentication where the Authentication and verification of the user is independent of whether it is inside of the network or outside. If any Inside Attacker may tries to attack victim uses his public key he may be restricted at the second factor authentication where any user needs to use smart card for the authentication.

$T_1 \rightarrow hash(ID_i)$, User A calculates hash over his Identity

$T_2 \rightarrow hash(ID_i||PW_i)$, User A calculates hash over concatenation of his Identity and password

$T \rightarrow (T_1, T_2)$, tupple is created from both hash values

$E_i \rightarrow E_T \rightarrow S$, tupple is then Encrypted using Elliptic Curve Cryptography and send to server

$Attacker_i \rightarrow sniffs\ (ID_i)\ and\ PW_i$, Attacker sniffs Identity and Password of User A

Attacker when tries to attack Server using the Identity of User A then Server will refuse since User A is already registered and ask for Smart Cards based authentication.

5.4.4 Outsider Attacks

The planned procedure implemented is based on 2 Factor Authentication where the Authentication and verification of the user is independent of whether it is inside of the network or outside. If any outside Attacker may tries to attack victim using public key of any user or any unwanted key he may be restricted at the second factor authentication where any user needs to use smart card for the authentication.

$T_1 \rightarrow hash(ID_i)$, User A calculates hash over his Identity

$T_2 \rightarrow hash(ID_i||PW_i)$, User A calculates hash over concatenation of his Identity and password

$T \rightarrow (T_1, T_2)$, tupple is created from both hash values

$E_i \rightarrow E_T \rightarrow S$, tuple is then Encrypted using Elliptic Curve Cryptography and send to server

$Attacker_i \rightarrow sniffs\ (ID_i)\ and\ PW_i$, Attacker sniffs Identity and Password of User A

Attacker when tries to attack User A for Identity and Password can't attack since the tuple is in Encrypted form and difficult to Decrypt.

5.4.5 Eavesdropping Attack

The attacker could change a victim's contact data to trick the victim's contacts into sending sensitive data to the attacker, but the Attacker when tries to Authenticate at the Server he failed to authenticate himself.

5.4.6 Eurograbber Attack

In this type of attack when Trojan's contaminate the User's mainframe and the occurrence witches communiqué with the series. In the Additional point aggressor recover the

operator's mobile quantity and contaminate the mobile maneuver. In the next chapter the following time the operator fuels into the bank version, the aggressor recruits a transmission of reserves from the user's explanation to the "mule" explanation. In the last point Bank directs a Contract Agreement Quantity via SMS.

Even though the Eurograbber Attack sniffs our First Factor Authentication but failed to authenticate during Second Factor, since it required Smart Cards for authentication and some computations needs to be performed by the User to issue these Smart Cards.

Table 5.1: Prevention of various attacks.

Replay Attack	Identity Disclosure Attack	Insider Attack	Outsider Attack	Eavesdropping	Identity Spoofing	Password based Attack	Man in the middle Attack	Eurograbber Attack
YES	YES	YES	YES	YES	YES	YES	YES	YES

The table 5.2 shows the analysis of Storage Cost in bits during First Factor Authentication and overall time taken to generate the token. The Computation of Storage Cost in our scheme can be calculated as:

$$N_t = hash(C_i)(1)$$

$$N_s = hash(C_i) + hash(PW_i) \qquad (2)$$

Where,

$$N_t = No.of\ bits\ in\ token$$

$$C_i = Challenge\ value\ from\ User\ i$$

$$N_s = No.of\ bits\ in\ Secrete\ Value\ during\ First\ Factor\ Authentication$$

$$PW_i = Password\ value\ of\ User\ i$$

Table 5.2: First Factor Authentication

No. of bits in token	No. of bits in conceal value	Time taken
32 bits	64 bits	11.538 sec

The table 5.3 shows the analysis of Storage Cost in bits at the Smart Card and at the Server Side. The analysis done here is on the basis of R. Song et. al's and the proposed scheme implemented. The proposed scheme implemented takes less storage cost at the smart card and server side. The computation of storage cost in our scheme can be calculated as -

$$T_s = PA_i + PB_i + PC_i + PD_i \qquad (1)$$

$$T_{s'} = T_s + X_s + ID_i + PW_i \qquad (2)$$

Where,

$$T_s = Total\ Storage\ Cost\ at\ Smart\ Card$$

$$PA_i = Hash(ID_i).xor.hash(X_s||hash(ID_i))$$

$$ID_i = Identity\ of\ User\ i$$

$$X_s = Secrete\ Key\ of\ Server$$

$$PB_i = PA_i.xor.hash(ID_i||PW_i)$$

$$PC_i = hash(PA_i)$$

$$PD_i = hash(ID_i||PW_i).xor.hash(X_s)$$

$$T_{s'} = Total\ Storage\ at\ Server$$

$$PW_i = Password\ of\ User\ i$$

Table 5.3: Storage judgment of the planned scheme

Storage/ scheme	Our scheme	R. song et. al's
Smart card	269 bits	320 bits
Server	372 bits	480 bits

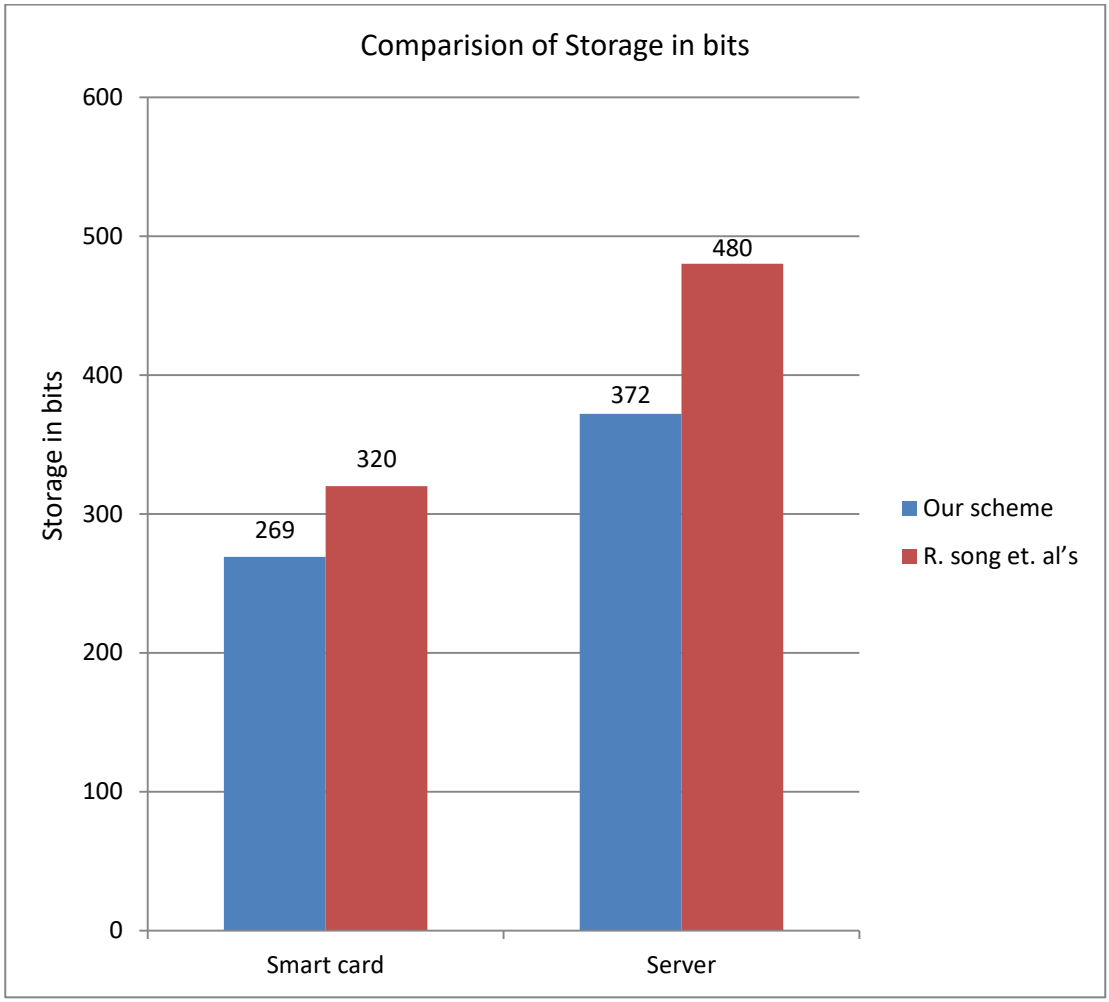


Figure 5.13: Comparison of Storage in bits

5.5 ANALYSIS OF COMPUTATIONAL COST

Total Computational Cost for First Factor Authentication

The Planned procedure implemented here is based on the Concept of Two Factor Authentication to provide Security of Online Web Transactions. Hence during the Communication from Sender to Receiver or from Client to Server requires some Data to be Stored at the Client or at the Server Side. Let us consider for Single User 'Ui' Transaction on Web, so during First Factor Authentication User 'Ui' stores his Challenge Value 'Ci' and password 'Pi. Here in the First factor Authentication the Overall Computational Cost at the Client Side will be:

$$C_{Ui} = C_{Ci} + C_{Pi}$$

Where,

C_{Ui} : Overall Computational Cost at the Client Side in bits.

C_{Ci} : Overall Computational Cost of the Challenge Value at Client Side in bits.

C_{Pi} : Overall Computational Cost of the Password at Client Side in bits.

Similarly at the Server Side the Overall Computational Cost at the Server Side will be:

$$C_{Si} = C_{pi}$$

Where,

C_{Si} : Overall Computational Cost at the Server Side in bits.

C_{Pi} : Overall Computational Cost of the Password at Server Side in bits.

Hence, overall Computational Cost for the First Factor Authentication will be

$$C_1 = C_{Ui} + C_{Si}$$

Where, C_1 : Overall Computational Cost for the First Factor Authentication.

Total Computational Cost for Second Factor Authentication

Second Factor Authentication consists of Four Phases; hence overall computational cost at each stage of the algorithm is given as:

During the registration phase when a new registration is send to Server and Server generates a Smart Card based on request, hence overall computational cost at the registration will be:

$$C_{ss} = C_A + C_B + C_C + C_D$$

Where,

C_{ss} : Overall computational cost for smart card storage in bits.

C_A : Overall computational cost for Parameter A in bits

C_B : Overall computational cost for Parameter B in bits

C_C : Overall computational cost for Parameter C in bits

C_D : Overall computational cost for Parameter D in bits

$$C = C_1 + C_{ss}$$

Where,

C: Overall Computational Cost in bits.

C_{ss} : Overall computational cost for smart card storage in bits.

C_1 : Overall Computational Cost for the First Factor Authentication.

The Table 5.4 is the analysis of the overall Computation cost by the planned procedure for number of Users. The Computational Cost for the No. of Users is less than the existing methodologies used for the Security prevention from various attacks.

Table 5.4: Analysis of Computational Costs on bits

No. of Users	Computational Cost in bits
5	461
10	532
15	680
20	811
25	925
30	1051
35	1245
40	1377
45	1475
50	1543

The Figure 5.14 is the analysis of the overall Computation cost by the planned procedure for number of Users. The Computational Cost for the No. of Users is less than the existing methodologies used for the Security prevention from various attacks.

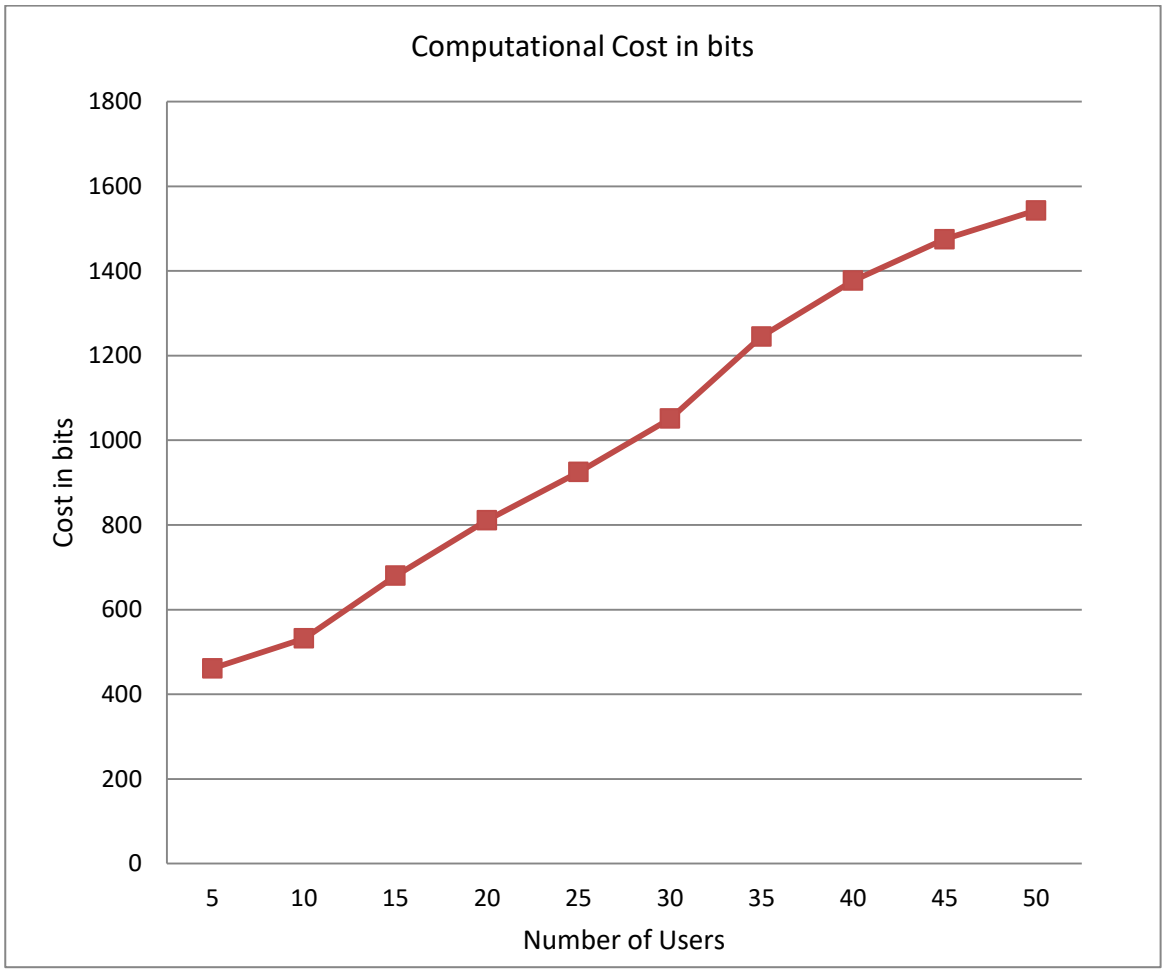


Figure 5.14: Comparison of Computational Cost in bits

5.6 ANALYSIS OF COMPUTATIONAL TIME

Computational time can be computed on the basis of communication time takes places at the First Factor and second factor Authentication.

$$T = T_1 + T_2$$

Where,

T: Overall Communication Time in ms

T1: Overall Communication Time for First Factor Authentication in ms.

T2: Overall Communication Time for Second Factor Authentication in ms.

However, Communication Time can be computed as the overall time algorithm will takes during sending and receiving of data from Client to Server or from Server to Client.

The Table 5.5 is the analysis of the overall Communication time by the planned procedure for number of Users. The Communication Time for the No. of Users is less than the existing methodologies used for the Security prevention from various attacks.

Table 5.5: Analysis of Communication Time in ms

No. of Users	Communication Time in ms
5	261
10	479
15	611
20	771
25	894
30	951
35	1050
40	1350
45	1528
50	1733

The Figure 5.15 is the analysis of the overall Communication time by the planned procedure for number of Users. The Communication Time for the No. of Users is less than the existing methodologies used for the Security prevention from various attacks.

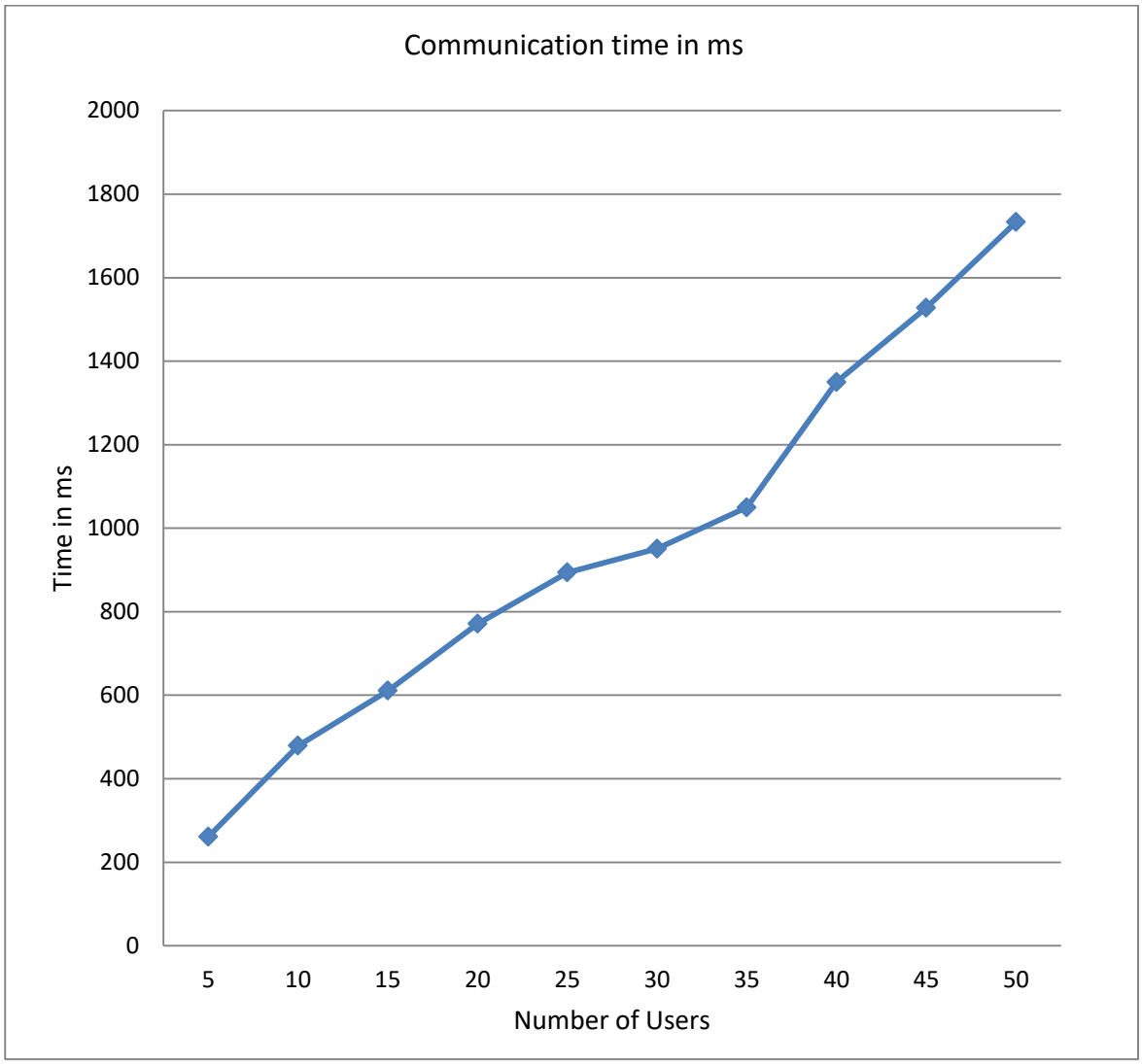


Figure 5.15: Comparison of Communication Time in ms

CHAPTER 6

CONCLUSION

6.1 CONCLUSION

Security in various E-commerce Applications includes an efficient framework in Information Security especially in Data and Computer security and other Online transactions in E-commerce applications. Security in E-Commerce application plays an important role for the secure and scalable transaction which includes various dimensions such as security-integrity, Confidentiality, Non-repudiation, Privacy etc. Hence for the Security of Online Transactions in E-Commerce based application various Security algorithms are implemented. Although these Security algorithms are efficient and provides Security from attacks but Data Storage during the transactions and Computational time of the algorithms is also imperative. Hence an efficient algorithm is implemented which provides Security in Online E-Commerce transactions and also provides efficient Computational Cost and time.

The planned procedure implemented here works on the framework of Authentication on Two Factor which provides Security from attacks especially in Online Web Transactions. The Methodology implemented works on two phases 1) Assigning the validity of the User by allocating a challenge value 2) Improved Smart Card based Authentication using Elliptic Curve based Encryption and Data Validation. The proposed technique implemented here prevents from numerous types of security attacks such as replay attack and identity disclosure attack or outsider attack and provides security from various dimensions such as security-integrity, Confidentiality, Non-repudiation, Privacy etc. The two factor verification that we proposed here takes low Computational Cost and Computational Time.

The planned procedure when implemented on Applications such as E-Commerce based Online Transactions in Web Mining it provides Security from various attacks such as Replay Attacks, Identity Disclosure Attack, Insider Attack, Outsider Attack, Identity Disclosure Attack and Man-in the Middle Attack.

The Methodology when applied on the quantity of customer / Users such as 5,10,15,20,25,30,35,40,45,50 it performs come computation at the Sender Side and Server Side and takes 461,532,680,811,925,1051,1245,1377,1475,1543 Computational Cost in bits and 261,479,611,771,894,951,1050,1350,1528,1733 Communication Time in milliseconds.

6.2 ADVANTAGES

1. Provides Security from security attacks in E-Commerce based Online Transactions.
2. Implementation of Authentication using Two Factorso that chances of fraud detection get minimized and Secrecy and Privacy is maintained.
3. The Methodology implemented takes less storage and Computational Cost from server side.
4. Provides less computational time.
5. The chief advantage of this explanation is that it delivers each user with the competence of collaborating steadily with other users in the system while only requiring it to remember a distinct password. This appears to be a more accurate situation in repetition than the one in which operators are probable to share multiple keywords, one for each gathering with which it may interconnect confidentially.

REFERENCES

1. XunYi,“Security Analysis of Yang et al.'s Practical Password-Based Two-Server Authentication and Key Exchange System”, 4th International Conference. Network and System Security (NSS), 2011.
2. N. Kuruwitaarachchi, P.K.W. Abeygunawardena, L.Rupasingha&S.W.I.Udara, “A Systematic Review of Security in Electronic CommerceThreats and Frameworks”, Global Journal of Computer Science and Technology: E Network, Web & Security Volume 19 Issue 1 Version 1.0, 2019.
3. HayaAlshehri, FaridMeziane, "The Influence of Advanced and Secure E-Commerce Environments on Customers Behaviour: The Case of Saudis in the UK," in 12th International Conference for Internet Technology and Secured Transactions, 2017.
4. Jiang Huiping. “Strong password authentication protocols”,4th International Conference Distance Learning and Education (ICDLE),2010.
5. Dr. Happy Agrawal, Moon MoonLahiri, “Gender Influenced Online Shopping Behavior among College Students”, Purakala (UGC Care Journal), Vol-31-Issue-55-June -2020
6. ShuoZhai,“Design and implementation of password-based identity authentication system”, 2010 International Conference Computer Application and System Modeling (ICCASM), 2010.
7. Harold NguegangTewamba, Jean Robert Kala Kamdjoug, Georges Bell Bitjoka, Samuel FossoWamba, Nicolas NkondockMiBahanag, “Effects of Information Security

Management Systems on Firm Performance", American Journal of Operations Management and Information Systems, volume 4(3): pp. 99-108, 2019.

8. Maithili Narasimha and Gene Tsudik. DSAC: integrity for outsourced databases with signature aggregation and chaining. Technical report, 2005.
9. PuspaIndahatiSandhyaduhita, "Supporting and Inhibiting Factors of E-Commerce Adoption: Exploring the Sellers Side in Indonesia," in International Conference on Advanced Computer Science and Information Systems, 2016.
10. Joseph, Randy Katz, Above the Clouds: A Berkeley View of Cloud Computing, University of California Electrical Engineering & Computer Science, February 10th, 2009.
11. Abdul Gaffar Khan, "Electronic Commerce: A Study on Benefits and Challeges in an Emerging Economy," Global Journal of Management and Business Research: B Economics and Commerce, vol. 16, no. 1, 2016
12. Patel, Chandrakant D., Shah, Amip J., "Cost Model for Planning, Development, and Operation of a Data Center," Internet Systems and Storage Laboratory, HP Laboratories, Palo Alto, June 9, 2005.
13. SomdechRungsrisawat, ThanapornSriyakul, KittisakJermsittiparsert, "The Era of e-Commerce & Online Marketing: Risks Associated with Online Shopping", International Journal of Innovation, Creativity and Change, Volume 8, Issue 8, 2019.
14. Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011.

15. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable Data Possession at Untrusted Stores,” Proc. 14th ACM Conf. Computer and Comm. Security (CCS ’07), pp. 598-609, 2007
16. H. Shacham and B. Waters, “Compact Proofs of Retrievability,” Proc. Int’l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (Asiacrypt), vol. 5350, pp. 90-107, Dec. 2008.
17. Cong Cao, Jun Yan, Mengxiang Li, "The Effects of Consumer Perceived Different Service of Trusted Third Party on Trust Intention: An Empirical Study in Australia," in 14th IEEE International Conference on e-Business Engineering, 2017.
18. D. Agrawal and C.C. Aggarwal, “On the Design and Quantification of Privacy Preserving Data Mining Algorithms,” Proc. 20th ACM SIGMOD-SIGACT-SIGART Symp. Principles of DatabaseSystems (PODS ’01), pp. 247-255, May 2001.
19. R. Agrawal and R. Shrikant, “Privacy Preserving Data Mining,”, Proc. ACM SIGMOD Int’l Conf. Management of Data 2000.
20. SheshadriChatterjee, "Security and Privacy Issues in E-Commerce: A Proposed Guidelines to Mitigate the Risk," in IEEE International Advance Computing Conference, 2015.
21. Revathi C, Shanthi K, Saranya A.R, "A Study on ECommerce Security Issues," International Journal of Innovative Research in Computer and Communication Engineering, vol. 3, no. 12, December 2015.
22. Y. Lindell and Benny Pinkas, “Privacy Preserving Data Mining”, Proc. Int’l Cryptology Conf. (CRYPTO), 2000.

23. SomdechRungsrisawat, WatcharinJoemsittiprasert, KittisakJermsittiparsert, " Factors Determining Consumer Buying Behaviour in Online Shopping", International Journal of Innovation, Creativity and Change, Volume 8, Issue 8, 2019.
24. Verykios V.S., Bertino E., Fovino I.N., Provenza L.P., Saygin, Y. &Theodoridis Y.(2004a). State-of-the-art in privacy preserving data mining, SIGMOD Record, Vol. 33, No. 1, pp.50-57.
25. Ghada El Haddad, EsmaAimeur, HichamHage, "Understanding Trust, Privacy and Financial Fears in Online Payment," in 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications, 2018.
26. "Trends in e-commerce & digital fraud: Mitigating the risks," EKN, 2017.
27. Lindell Y. &Pinkas B.(2009). Secure Multiparty Computation for Privacy-Preserving Data Mining, Journal of Privacy and Confidentiality, Vol 1, No 1, pp.59-98.
28. S. Papadimitriou, F. Li, G. Kollios, and P.S. Yu, "Time Series Compressibility and Privacy," Proc. 33rd Int'l Conf. Very Large Data Bases (VLDB '07), 2007.
29. F. Li, J. Sun, S. Papadimitriou, G. Mihaila, and I. Stanoi, "Hiding in the Crowd: Privacy Preservation on Evolving Streams Through Correlation Tracking," Proc. IEEE 23rd Int'l Conf. Data Eng. (ICDE), 2007.
30. O. Goldreich. Foundations of Cryptography, Volume 2. Cambridge University Press, 2004.
31. J. Yedidia, W. Freeman, and Y. Weiss. Understanding belief propagation and its generalizations. In Exploring Artificial Intelligence in the New Millennium. Morgan Kaufmann, 2003.

32. Chen, C.L., Lu, M.S., Guo, Z.M.: A non-repudiated and traceable authorization system based on electronic health insurance cards. Journal of Medical Systems pp. 1–12, doi: 10.1007/s10916-011-9703-4, 2011.
33. Huang, X., Xiang, Y., Chonka, A., Zhou, J., Deng, R.: "A generic framework for three-factor authentication: preserving security and privacy in distributed systems. Parallel and Distributed Systems", IEEE Transactions on 22(8), 1390–1397, 2011.
34. Chen, T., Hsiang, H., Shih, W.: "Security enhancement on an improvement on two remote user authentication schemes using smart cards", Future Generation Computer Systems 27(4), 377–380, 2011.
35. Chen, Y.L., Chou, J.S., Huang, C.H.: "Improvements on two password-based authentication protocols". Cryptology ePrint Archive, Report 2009/561, http://eprint.iacr.org/2009/561.pdf, 2009.
36. Khan, M., Kim, S., Alghathbar, K.: Cryptanalysis and security enhancement of a more efficient & secure dynamic id-based remote user authentication scheme'. Computer Communications 34(3), 305–309, 2011.
37. Li, C.T., Lee, C.C.: "A robust remote user authentication scheme using smart card" Information Technology And Control 40(3), 236–245, 2011.
38. AdiSantoso, UtikBidayati, Hendar, "Factors Influencing Online Purchase Intention: A Consumer Behavioral Study on Indonesia", International Journal of Innovation, Creativity and Change, Volume 9, Issue 5, 2019.
39. Ma, C.G., Wang, D., Zhang, Q.M.: "Cryptanalysis and improvement of sood et al.s dynamic id-based authentication scheme", In: Ramanujam, R., Ramaswamy, S. (eds.) ICDCIT'12, LNCS, vol. 7154, pp. 141–152. Springer-Verlag, 2012.

40. Kasper, T., Oswald, D., Paar, C.”Side-channel analysis of cryptographic rfids with analog demodulation”. In: Juels, A., Paar, C. (eds.) RFIDSec’12, LNCS, vol. 7055, pp. 61–77. Springer Berlin / Heidelberg, 2012.
41. Pu, Q.,”An improved two-factor authentication protocol”. In: 2010 International Conference on Multimedia and Information Technology (MMIT). vol. 2, pp. 223– 226. Ieee, 2010.
42. Shim, K.:” Security flaws in three password-based remote user authentication schemes with smart cards”.Cryptologia 36(1), 62–69, 2012.
43. Wang, Y.G.: “Password protected smart card and memory stick authentication against off-line dictionary attacks”. In: Gritzalis, D., Furnell, S., M., T. (eds.) SEC 2012, IFIP AICT, vol. 376, pp. 489–500. Springer Boston availe at http://coitweb.uncc.edu/ yonwang/papers/smartcard.pdf, 2012.
44. Xie, Q.: Dynamic id-based password authentication protocol with strong security against smart card lost attacks. In: Snac, P., Ott, M., Seneviratne, A., Akan, O. (eds.) Wireless Communications and Applications, LNICST, vol. 72, pp. 412–418. Springer Berlin / Heidelberg, 2012.
45. Whitfield Diffie and Martin Hellman. New directions in cryptography. IEEE Trans. Inf. Theory., 22(6):644-654, September 2006. pages 47, 51
46. J. M. Park, E. Chong, H. J. Siegel, and I. Ray “Constructing fair exchange protocols for e-commerce via distributed computation of RSA signatures,” in Proceedings PODC’03, pp. 172–181, ACM Press, 2003.

47. Ying Zhang, Chenyi Zhang, Jun Pang and SjoukeMauw “Game-Based Verification of Multi-Party Contract Signing Protocols”, Formal Aspects in Security and Trust, Lecture Notes in Computer Science, Volume 5983, pp 186-200, 2010.
48. M. Choudary Gorantla, Colin Boyd, and Juan Manuel Gonzalez Nieto. Modeling key compromise impersonation attacks on group key exchange protocols. In Proceedings of the 12th International Conference on Practice and Theory in Public Key Cryptography: PKC '09, pages 105-123, Berlin, Heidelberg, 2009. Springer-Verlag. pages 51, 80, 82,83, 84, 85, 92
49. Emmanuel Bresson, Olivier Chevassut, and David Pointcheval. Provably authenticated group Diffie-Hellman key exchange - The dynamic case. In Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology, ASIACRYPT '01, pages 290{309, London, UK, 2001. Springer-Verlag. pages 52, 79, 87
50. Rolf Blom. An optimal class of symmetric key generation systems. In Proc. of the EUROCRYPT'84 workshop on Advances in cryptology: theory and application of cryptographic techniques, pages 335{338, New York, USA, 1985. Springer-Verlag New York, Inc. pages 49.
51. Emmanuel Bresson and Mark Manulis. Securing group key exchange against strong corruptions. In Proceedings of the 2008 ACM symposium on Information, computer and communications security, ASIACCS '08, pages 249{260, New York, USA, 2008. ACM. pages 51, 52, 53, 79, 80, 83, 85, 86.

52. Yair Amir, Yongdae Kim, Cristina Nita-Rotaru, and Gene Tsudik. On the performance of group key agreement protocols. ACM Trans. Inf. Syst. Secur., 7(3):457{488, August 2004. pages 47.
53. J. Katz, R. Ostrovsky, and M. Yung: “Efficient And Secure Authenticated Key Exchange Using Weak Passwords”. Journal of the ACM, 57(1):78–116, 2009.
54. A. Groce, J. Katz: “A New Framework For Efficient Password-based Authenticated Key Exchange”. In: 17th ACM Conf. on Computer and Communications Security, pp. 516–525. ACM Press, New York, 2010.
55. CosmasAnayochukwuNwankwo, MacDonald Kanyangale and James OkechukwuAbugu, “Online Shopping Industry and Its Consumers in Nigeria”, Journal of Economics, Management and Trade volume 24(3), pp. 1-12, 2019.
56. J. Katz and V. Vaikuntanathan: “Password-based Authenticated Key Exchange Based on Lattices”. In: Advances in Cryptology, Asiacrypt 2009, volume 5912 of LNCS, pp. 636–652. Springer, 2009.
57. S. Wanga, Z. Cao, K.-K. Choo, and L. Wang, "An improved identitybased key agreement protocol and its security proof," An International Journal of Information Sceinces, vol. 179, pp. 307-318, January. 2009.
58. D. XiaoFei and M. ChuanGui, "Cryptoanalysis and Improvements of Cross-Realm C2C PAKE Protocol,"WASE09, procedings of IEEE, International Conference on Information Engineering, pp. 193-196, 2009.
59. Dr. GarimaSinha, Dr. Deepak Kumar Sinha, FeiduAkmel, AmareMulatie, “Effect of IT and Mobile Infrastructures on the Online Business in Ethiopia: Trends, Opportunities

and Issues", IOSR Journal of Mobile Computing & Application (IOSR-JMCA) Volume 3, Issue 2. PP 23-30, 2016.

60. Pu, Q.,"An improved two-factor authentication protocol". In: 2010 International Conference on Multimedia and Information Technology (MMIT). vol. 2, pp. 223– 226. Ieee, 2010.
61. Wang, Y.G.: "Password protected smart card and memory stick authentication against off-line dictionary attacks". In: Gritzalis, D., Furnell, S., M., T. (eds.) SEC 2012, IFIP AICT, vol. 376, pp. 489–500. Springer Boston availe at http://coitweb.uncc.edu/ yonwang/papers/smartcard.pdf, 2012.
62. Xu, J., Zhu, W., Feng, D.:" An improved smart card based password authentication scheme with provable security". Computer Standards & Interfaces 31(4), 723–728, 2009.
63. Ms. Palak Gupta, Dr. AkshatDubey, "E-CommerceStudy of Privacy, Trust and, Security from Consumer's Perspective" International Journal of Computer Science and Mobile Computing, vol. 5, no. 6, pp. 224-232, June 2016.
64. Abdullah, MadihahMohd Saudi and NorBadrulAnuar, "Mobile Botnet Detection: Proof of Concept", 2014 IEEE 5th Control and System Graduate Research Colloquium, 2014.
65. K. Nirmal, S.E. Vinodh Edwards, K. Geetha, " Maximizing Online Security by providing a 3 Factor Authentication System to counter-attack Phishing", IEEE 2010.
66. NikAlifAmriNikHashimet. al, "Internet Shopping: How the Consumer Purchase Behaviour is Impacted by Risk Perception", Test Engineering and Management,

Published by: The Mattingley Publishing Co., Inc., Volume 59 Issue 6s Page Number: 1014- 1021, 2019.

67. Mohammad Irshad, "A Systematic Review of Information Security Frameworks in the Internet of Things," in IEEE 18th International Conference on High Performance Computing and Communications, 2016.

PUBLICATION FROM THIS WORK

1. Mohammad Salman Husain, Dr. Mohammad Haroon, 'An Enriched Information Security Framework from Various Attacks in the IoT', In International Journal of Innovative Research in Computer Science & Technology (IJIRCST), Volume-8, Issue-4, July-2020.
2. Mohammad Salman Husain, Dr. Mohammad Haroon, 'A Review of Information Security from Consumer's Perspective Especially in Online Transactions', In International Journal of Engineering and Management Research", Volume-10, Issue-4, August 2020.

International Journal of Engineering and Management Research e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-10, Issue-4 (August 2020)
www.ijemr.net https://doi.org/10.31033/ijemr.10.4.2

A Review of Information Security from Consumer's Perspective Especially in Online Transactions

Mohammad Salman Husain[1] and Dr. Mohammad Haroon[2]
[1]PG Scholar, Department of Computer Science & Engineering, Integral University, Lucknow, INDIA
[2]Associate Professor, Department of Computer Science & Engineering, Integral University, Lucknow, INDIA

[1]Corresponding Author: salmank094@gmail.com

ABSTRACT

In the current internet technology, most of the transactions to banking system are effective through online transaction. Predominantly all these e-transactions are done through e-commerce web sites with the help of credit/debit cards, net banking and lot of other payable apps. So, every online transaction is prone to vulnerable attacks by the fraudulent websites and intruders in the network. As there are many security measures incorporated against security vulnerabilities, network thieves are smart enough to retrieve the passwords and break other security mechanisms. At present situation of digital world, we need to design a secured online transaction system for banking using multilevel encryption of blowfish and AES algorithms incorporated with dual OTP technique. The performance of the proposed methodology is analyzed with respect to number of bytes encrypted per unit time and we conclude that the multilevel encryption provides better security system with faster encryption standards than the ones that are currently in use.

Keywords-- Online Transaction, Blowfish Algorithm, AES Algorithm, Dual OTP, Banking System

I. INTRODUCTION

In order to provide security to the customer, existing banking system uses various levels of security mechanisms. Even though tough encryption standards are provided against network attacks, it is prone to be broken. Intruders are smart enough to retrieve the passwords of the customers through online transaction. As per the world payments report, in current technology people prefer to use cashless payments rather than the cheques or cash payments. As we all know that these kinds of e-transactions provide huge number of benefits to the customers for example, by making the transactions easier, faster and instant payments. Overall, as per the survey an Indian uses online transaction system once in a week for payment. This online transaction might be through credit/debit cards, e-wallets, UPI's, food cards, travel cards and some authorized e-payment systems.

Many security implementation methods like hardware level security, antivirus, anti- malware and antispyware programs, strong passwords, single time bound OTP system, virtual private network, secured site uses SSL certificate are used in practice. However, in spite of all these security mechanisms intruders go for brute force attempts to decrypt the PIN numbers and passwords etc. So, single level encryption standard is not sufficient to provide high level security for online transaction system. At present we need to have a multilevel encryption standard wherein even if anyone encryption standard is broken, the online transaction requested by the customer will be completed with the other Encryption standard. Our paper focuses on multilevel security with Blowfish and AES algorithm along with dual OTP scheme which may lead to stronger level of protection against threat encountered in online transactions. The paper has been organized as follows: Section II describes about the related work and section III depicts the proposed system of security. Section IV deals with experimental results and finally section V concludes the paper.

II. RELATED WORK

In [1], the different methodologies adopted for e-transactions security in mobile devices against security threat has been discussed which has severe drawback over multi-level transactions. Using longitude and latitude [2], according to the location high level authentication has been incorporated to overcome the intruder attack in network transactions. The various privacy risks and their impact [3] on mobile payment services are extensively focused and various limitations also depicted to create awareness among customers of online transactions. In [4], two factor security model based on QR based login system is discussed and it has limitation over scanning of QR code. Innovation in mobile wallets [5] has been arised in e-commerce services and its impact and security over the communication network and banking system is also under research against malicious attacks. At current scenario, a more secured mechanism is vital for online transaction and one such method is visual cryptographic methods [6] for e-commerce system which is less vulnerable to attacks. Apart from password-based authentication, more reliable future protection mechanisms against electronic payment attacks are discussed by the paper Jeffus et al [7]. A method of data mining security [8] using privacy preserving is another context of data extraction in the internet. In this paper [9], every transaction sent by the customer is wrapped around an image and has been shown with improved efficiency against security attacks.

In [10], a new methodology of steganography with images has been proposed which is shown to be having less amount of data transfer between merchant and the customer. A mobile based E-Wallet [11], is an innovative method incorporated in the e-world which is assumed to be less time consuming. Banking and financial institution [12] is actually influenced by the most of the advancements in science and technology.

III. PROPOSED METHODOLOGY

A. Blowfish and AES Algorithms

For the multilevel security implementation, blowfish algorithm found to be the better performance-oriented algorithm due to the low block size. In the context of this paper, as we use multilevel security mechanism, in the first level if there is any e-transaction between the intra banking system, then Blowfish algorithm has been incorporated which is found to be less time-consuming process. In the second level when there is a transaction between a host of one bank and the host of another bank then it is desired to incorporate high level of security and that is the place, we put in forth the AES authentication mechanism.

B. Dual OTP Strategy

Apart from the two-level authentication, one more security mechanism with respect to dual OTP also imposed in the proposed methodology. With this method, all the banking customers are supposed to have two mobile numbers. First primary number will be the customer number and the secondary number is the confidante that the customer provides when registering with the bank. Both these OTPs shall together validate the transaction. Failure to provide even one of them will see the transaction fail. Using this strategy an added measure of security can be incorporated into the system.

C. Transaction

When the client makes contact for a transaction, the server needs to check whether the transaction is intra-bank or inter-bank. If the transaction is intra-bank, blowfish is set as the encryption standard. However, if the transfer is to a different bank, the standard is set to AES.

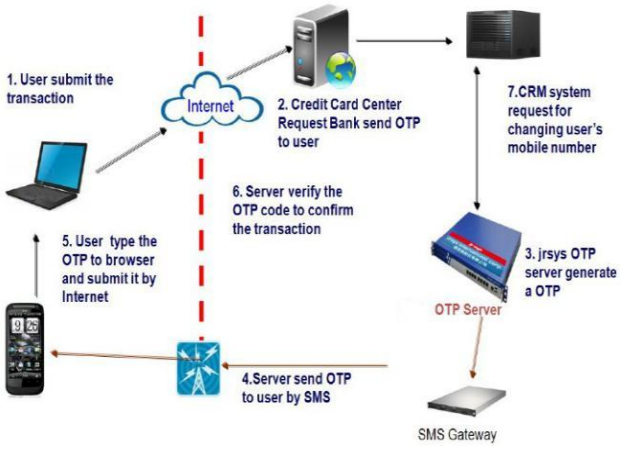


Figure 1: Banking Transaction

An example online banking transaction is shown in figure1 that involves server authentication. First step of transaction is user authentication followed by server verification and finally OTP generation. Then the user is allowed to make the payment for the e-commerce websites.

IV. RESULT ANALYSIS

The performance of the proposed algorithm is measured with the help of core i3,7th generation machine with JDK implementation and a database backend for storing user information.

The performance of the blowfish and AES encryption standards with respect to number of bytes encrypted is shown in table I and II.

Table 1: Blow Fish Performance

Time Elapsed(s)	Bytes Encrypted
136	137325
158	158959
162	1663634
176	191383
219	232398

The time taken for encryption is less and thus improves the performance of the banking system. Advanced encryption algorithms like RSA algorithm takes more time in the encryption process as it is involved with large prime number generation. In blowfish algorithm we use less rounds of computation and thus saves time of encryption and leading to fast access to banking system during online transaction.

Table 2: AES Performance

Time Elapsed(s)	Bytes Encrypted
136	137325
158	158959
162	1663634
176	191383
219	232398

Similarly, AES algorithm also provides greater time consumption in encryption process and thus gives speedy transaction. Although, AES is an ancient algorithm used for encryption the time elapsed for encryption still found to be better than the RSA algorithm.

The actual simulation of the transaction system starts with a new user registration page created wherein customers have to enter all the details about them and a new login will be created. When the customer wants to perform any online transaction, he has to go inside the login page. An implementation of the banking system is incorporated with a login page shown in figure2. Once the login page is created the customer details are registered in the banking system. All the user passwords are encrypted inside the database with blowfish algorithm.

Figure 2: Login Page

Once the user authentication is verified at the back end then the customer is allowed to access the entire features of banking system.

Figure 3: Transaction using OTP

While entering the customer details during registration, it is mandatory that two mobile numbers are required from the customer side: primary number and a secondary confidante number. The strategy of dual OTP is incorporated with these two phone numbers. The innovation in multi level encryption is the generation of this dual OTP. The dual OTP generated during the customer online transaction is shown in figure3. This security system improves the performance against threats that is a major concern in online transactions.

Figure 4: OTP Verification

As per the dual OTP strategy, first OTP will be generated to the customer primary mobile as shown in figure 4, which has to be initially validated against the banking server.

The main focus on this kind of new mechanism is to give the online transaction users the facilities to perform the transaction easily without any complexities [13]. As per our proposed system, we find performance improvement not only in security but also with respect to faster access of transaction over the online banking system.

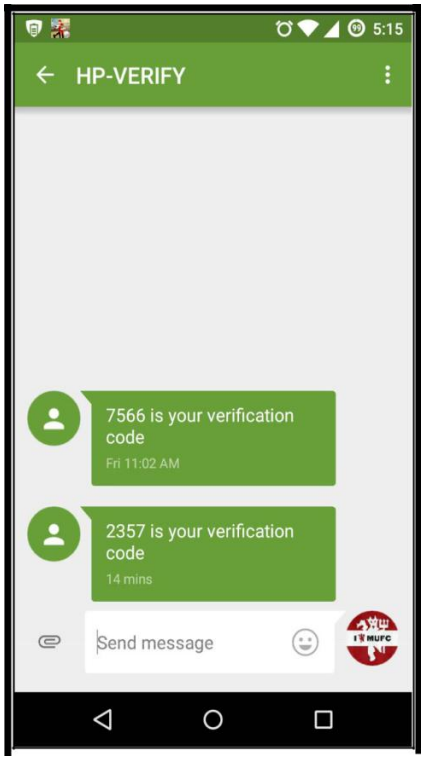


Figure 5: Dual OTP Verification

Later, the second OTP will be generated (figure5) to the secondary mobile and both will be verified by the banking system. Once after the authentication from the bank, then the online transaction will be initiated.

V. CONCLUSION

As in the world of digitization, lot of attacks over E-transactions has been a greatest threat for e-commerce sites. Altogether both customers and banking security systems are affected through various malicious attacks by the intruders. Although huge security algorithms through various measures and means have been incorporated but still more authenticated services needed for transactions on internet. One such multilevel security mechanism has been imposed in this paper and provides more than 10% performance over time and security compared to existing algorithms. Dual OTP scheme is also one of the identified high security over one-time OTP system. In future more reliable visual cryptographic and time consuming steganography methods can be used in e-transactions.

REFERENCES

[1] F. Gao, P. L. P. Rau, & Y. Zhang. (2018). Perceived mobile information security and adoption of mobile payment services in China. *Mobile Commerce: Concepts Methodologies Tools and Applications*, 1179-1198.

[2] Dr. A.L.N Rao, Silky Puri, & Shalini Rana. (2013). Review: Location based authentication to mitigate intruder attack. *International Journal of Engineering and Innovative Technology (IJEIT), 2*(9), 336-339.

[3] V. L. Johnson, A. Kiser, R. Washington, & R. Torres. (2018). Limitations to the rapid adoption of M-payment services: Understanding the impact of privacy risk on M-Payment services. *Computers in Human Behavior, 79*, 111-122.

[4] Soonduck Yoo, Seung-jung Shin, & Dae-hyunRyu. (2013). An innovative two factor authentication method: The QR login system. *International Journal of Security and Its Applications, 7*(3), 293-302.

[5] S. Mittal, V. Kumar. (2018). Adoption of mobile wallets in india: an analysis. *IUP Journal of Information Technology, 14*(1), 42-57.

[6] M. Suresh, B. Domathoti, & N. Putta. (2015). Online secure e-pay fraud detection in e-commerce system using visual cryptographic methods. *International Journal of Innovative Research in Computer and Communication Engineering, 3*(8), 7519-7525.

[7] B. Jeffus, S. Zeltmann, K. Griffin, & A. Chen. (2017). The future of mobile electronic payments. *Journal of Competitiveness Studies, 25*(3-4), 216-223.

[8] R. Purohit & D. Bhargava. (2017). An illustration to secured way of data mining using privacy preserving data mining. *Journal of Statistics and Management Systems, 20*(4), 637-645.

[9] N. Shrivastaval & T. Verma. (2015). A survey on various techniques for generating image steganography with improved efficiency. *International Journal of Advanced Research in Computer Engineering & Technology, 4*(3), 1005-1009.

[10] S. Roy & P. Venkateswaran. (2014). Online payment system using steganography and visual cryptography. In: *Proceedings of the IEEE Conference on Electrical Electronics and Computer Science*, pp. 88-93.

[11] G. Kanimozhi & K. S. Kamatchi. (2017). Security aspects of mobile based e wallet. *International Journal on Recent and Innovation Trends in Computing and Communication, 5*(6), 1223-1228.

[12] Mr. Shakir Shaik & Dr. S.A. Sameera. (2014). Security issues in e-banking services in Indian scenario. *Asian Journal of Management Sciences, 02*(03), 28-30.

International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-8, Issue-3, May 2020
https://doi.org/10.21276/ijircst.2020.8.4.3
www.ijircst.org

An Enriched Information Security Framework from Various Attacks in the IoT

Mohammad Salman Husain, Dr. Mohammad Haroon

ABSTRACT- Security in various E-commerce Applications includes an efficient framework in Information Security especially in Computer Security, Data Security and other online transactions in E-commerce applications. Security in E-Commerce application plays an important role for the secure and scalable transaction which includes various dimensions such as security-integrity, Confidentiality, Non-repudiation, Privacy etc. Hence for the Security of Online Transactions in E-Commerce based application various Security algorithms are implemented. Although these Security algorithms are efficient and provides Security from various attacks but Data Storage during the transactions and Computational time of the algorithms is also important. The existing architecture proposed for the security of online e-transactions in web applications provides security from different attacks and is efficient in terms of computational parameters, but there are certain issues which need to be overcome such as: Security Prevention from different attacks during Online Transactions in Web Mining especially in E-commerce Applications, Increase use of Computational Cost at the Client and Server Side. The Proposed framework provides Security prevention from various attacks especially in IoT. The methodology implemented here works on the basis of authenticating the validity of the User by allocating a challenge value and hope that our proposed framework will be more effective and efficient.

KEYWORDS- Information Security, IoT, Computer Security, E-commerce, Authentication.

I. INTRODUCTION

The measures document two workers to produce a common, cryptographically robust important beached on an innovative, low-entropy, communal subversive (i.e., a watchword). The determination in this backdrop is to avert offline terminology occurrences where an adversary

Manuscript received 12 July, 2020.

Mohammad Salman Husain, PG Scholar, Department of Computer Sc. & Engineering, Integral University, Lucknow-India, (salmank094@gmail.com)

Dr. Mohammad Haroon, Associate Professor, Department of Computer Sc. & Engineering, Integral University, Lucknow India

systematically records probable keywords on its particular, undertaking to struggle the precise keyword to perceived etiquette employments. Coarsely, a PAKE technique is endangered if off-line sessions are of no practice and the unsurpassed measure is an online language dose somewhere an opponent necessity dynamically tries to reproduce an authentic gathering using each imaginable watchword. On-line doses of this category are distinguishing in the traditional of password-based authorization; more exceedingly, they can be identified by the waitperson as botched login efforts and fortified alongside. Procedures for reliable key disagreement license two festivities to harvest a mutual, cryptographically durable significant while cooperating over a self-doubting arrangement underneath the inclusive controller of a contestant [20]. Such etiquettes are between the most approximately used and indispensable cryptographic primitives; positively, procedure on a common important is desirable beforehand developed smooth responsibilities such as encoding and communication verification developed conceivable. PAKE measures document two workforces to harvest a shared, cryptographically robust key originated on an innovative, low-entropy, communal underground (i.e., a watchword). Unevenly, a PAKE method is endangered if off streak amounts are of no usage and the greatest incidence is an online vocabulary bout where an enemy must belligerently attempt to mimic an authentic gathering using each conceivable watchword. Online doses of this lesson are inherent in the standard of watchword founded authorization; more conspicuously, they can be distinguished by the waitperson as unsuccessful login exertions and fenced alongside [21]. Maximum watchword grounded user corroboration organizations residence whole belief on the verification waitperson where keywords or effortlessly resultant watchword confirmation statistics are stowed in a dominant folder [3, 19]. Traditional procedures for watchword grounded confirmation undertake a solitary waitron which supplies the entire evidence (e.g., the watchword) essential to confirm an operator. Watchword grounded corroboration is the maximum normally used object confirmation method, owing to the circumstance that no protected stowage is compulsory, and a operator solitary requirements to remember his watchword and then can authenticate wherever, anytime. Maximum of the prevailing watchword based proof arrangements commence the solitary

waitron standard wherever a solitary waitperson transpires in a society. The topmost badly-behaved of the solitary waitron conventional is that the attendant may moment in a solitary fact of devastation, in the wisdom that conciliation of the waitron exposures all manipulator watchwords apprehended by the waitron. Some normally used practices for watchword confirmation are conversed beneath [2, 5]:

A. Two Servers Password Authentication

Two server confirmation instruments are painstaking to be protected for confirming a user in Internet grounded atmosphere. As the quantity of amenities delivered operational is day by day snowballing, operators proposing to use numerous operational amenities are also cumulative. Finished each provision demanding the operator to greatest independently, the upstairs of remembering many employer (Uniqueness) ID /watchword pairs has led to the problematic of unforgettable. In this daily, planned a two-server password authentic key arrangement instrument using watchword where the employer wants to identify his clandestine key. The real-world two waitron watchword verification and key exchange organization that is protected in contradiction of disconnected glossary doses by waitrons once they are skillful by challengers [8, 10].

B. Quantum Channel for two Server Password Authentication

In significant cryptography, significant key circulation etiquettes employment dramatic instrument to allocate meeting answers and community deliberations to checkered for listeners and authenticate the accuracy of a conference significant. Though, communal deliberations necessitate additional communiqué circles among a dispatcher and earpiece and charge valuable quantum bits. The significant based two server keyword authentication procedure flow draw inaccessible and elucidates our construction of two server keyword scheme positioned using the quantum key classical to efficiently store user password in the internet applications. The greatest specimen of this two influence confirmation organization is our present ATM organization, in where the ATM valentine is one influence and the PIN quantity is additional influence. So if the ATM pass is misplaced wages, the validation functionality will be incapacitated. As distant as biometrics is worried, the refuge is self-same active and effectual in this organization ever the less the individual worries are the charge of hardware and software complexity.The waitron is bargained by incomes of a disconnected vocabulary spell. In fresh centuries, abundant courtesy has absorbed on conniving watchword based authentic crucial conversation procedures which can struggle any nice of interloper's dose. To crack this problematic, a new-fangled sympathetic of confirmation assembly baptized the numerous waitperson confirmations was planned. In these numerous server confirmation surroundings, the two-server confirmation etiquette [1] [4] is the humble stand the most satisfactory to users.

C. Two Server Systems

The notion of a manipulator id and watchword is a charge actual and well-organized technique. Recognizing and permitting the sanctioned operator to admittance the possessions is unique of the important characteristics of confirmation organization [7]. A solitary waitron organization is an organization in which the watchword will be kept in a lone waitron. Though seeing the confirmation organization grounded on a solitary waitron, nearby are approximately problems. The solitary waitron organization is susceptible to all categories of bouts from interlopers. The impostor can drudge the organization by tiresome all conceivable explanations till the organization gets cooperated is the maximum positive in the unsociable waitperson arrangement and thorough exploration also can be positive as publicized in Fig 1.

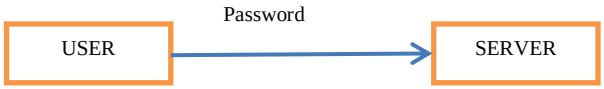


Fig 1: Block Diagram of a Single Server System

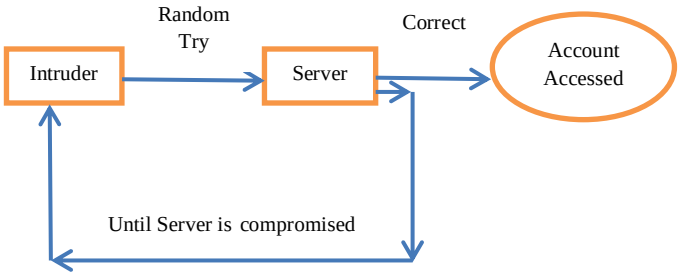


Fig 2: Example of single server system hacked by Intruder

Consequently, it's essential to familiarize the notion of two waitron confirmation organization. In the circumstance of a solitary waitron organization, the attackers can effortlessly negotiation. Nevertheless in the two waitron organization it would not be simply bargained by the aggressor.

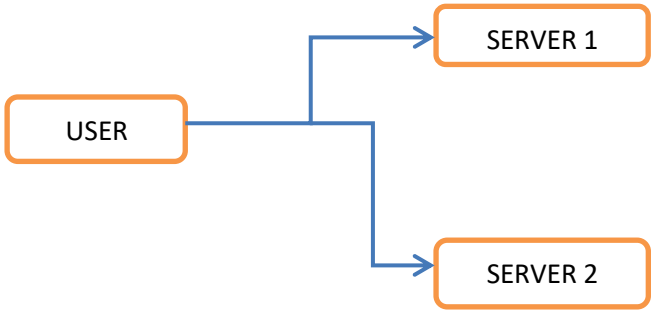


Fig 3: Block Diagram of Two Server System

II. LITERATURE REVIEW

Let's discuss works proposed by various researchers by S. Bellovin and M. Merritt gives the first fruitful password-authenticated key arrangement means were Encrypted Key Exchange means described. Although numerous of the first approaches were defective, the enduring and greater forms of EKE efficiently increase a shared keyword into a collective key, which can be used for encryption and/or message verification. Procedures for genuine key exchange permit two gatherings to produce a communal, cryptographically sturdy key while collaborating over an uncertain network below the comprehensive Regulator of an opponent. Such procedures are amongst the most extensively used and important cryptographic primitives; indeed, arrangement on a common key is essential before higher-level errands such as encoding and memorandum corroboration developed imaginable. Watch word grounded authentic important conversation measures document two operators to harvest a mutual, cryptographically-strong key originated on an original, low-entropy, common underground (i.e., a watchword). Katz, Ostrovsky, and Yung (KOY) [6] established the chief well-organized PAKE procedure with a resistant of refuge in the normal perfect. The technique was unconventional anxious by Gennaro and Lindell (GL), who contributed an overall outline that incorporates the innovative KOY procedure as a singular circumstance. These procedures are protected smooth underneath harmonized presentations by the similar get-together, but necessitate a shared orientation thread. Though this might be fewer attractive than the unadorned classical, dependence on a CRS prepares not seem to be a thoughtful disadvantage in repetition for the disposition of PAKE, where mutual strictures can be hard oblique into an application of the etiquette. The KOY/GL outline necessitates a CCA protected encoding arrangement (such as Cramer-Shoup cryptosystem with a connected straight projective hash connotation and its postponements necessitate four rounds in command to achieve common confirmation. Virtually all succeeding effort on well-organized PAKE in the normal prototypical can be watched as spreading and construction on the KOY/GL outline. Wanga, Z. Cao, K.-K. Choo, and L. Wangthe[9] first proper refuge classical for authentic key exchange conventions between two festivities. The latter has been extended to the password-based setting with security analyses of the above 2-party password-based key exchange, under idealized assumptions, such as the random oracle and the ideal cipher models. Password-based arrangements, provably protected in the normal classical, have been recently proposed but only for two parties. papers considered password-based protocols in the 3-party setting, but none of their schemes enjoys provable security. In fact, our general edifice appears to be the first provably-secure 3-party password-based authentic key exchange etiquette.

D. XiaoFei and M. Chuan Gui[11] introduce additional connected line of investigation is authenticated key conversation in the 3-party location. The primary exertion in this extent is the etiquette of Needham and Schroeder which stimulated the Kerberos disseminated organization. Later, Bellare and Rog away familiarized a prescribed refuge classical in this situation length ways with an edifice of the primary provably protected symmetric crucial grounded key circulation arrangement. In this weekly, we reflect the unusual but vital case in which the underground explanations are pinched from a unimportant set of ethics. Yang et al.'s [16] pointed out about arrangement is susceptible to important cooperation occurrence. Astonishingly, we originate Yang et al.'s arrangement still cannot accomplish its demanded foremost refuge goalmouth by representative a disconnected watchword predicting occurrence in Supplement A, and finished the refuge examination of Yang et al.'s arrangement, some refinements and contests in conniving this type of arrangements, dissimilar from the outdated watchword grounded confirmation, are exposed. Notwithstanding of this, Yang et al.'s prescribed adversary traditional does incarceration the scrupulous two influence corroboration of shrewd card-based keyword authorization preparations: only with both the clever card and the accurate keyword can a user communicate out the smart-card-based keyword authorization procedure absolutely with the isolated corroboration waitron. Xu, J., Zhu, W., Feng, D.[17] planned a general edifice agenda to adapt the conservative provably protected PAKE procedures to shrewd card-based forms and additional intentional an innovative arrangement to validate its efficacy. The new structure is demanded to be locked and can gratify all their projected principles. In the subsequent, we will expression that their outline is essentially disposed to disconnected keyword foreseeing occurrence, thus retreating the power completed that the new structure is protected smooth if the secret statistics packed in smart card is exposed by the opponent. Zubaile Abdullah, Madihah Mohd Saudi and Nor Badrul Anuar proposed a new and efficient technique for the Mobile Botnet Detection using Proof Concept [18]. This tabloid is offering an impermeable of notion on how the bot systems and the continuing exploration to perceive and answer to the movable botnet competently. Discovery of botnet spiteful movement is completed complete an investigation of Cruse wind Botnet cipher using opposite manufacturing development and stationary investigation practice.

III. METHODOLOGY

The Proposed methodology implemented here is based on the concept of authenticating the validity of the User by allocating a challenge value which provides Security prevention from various attacks especially in IoT. The Proposed methodology implemented works on the basis of the following -

- Whenever any new Customer performs any online Transaction on Web, he needs to do handshaking with the Server using shared Challenge value over secure channel. Handshaking between customer and server is done based on challenge value and secrete Shared Password. The Challenge value is limited for a particular Session only.
- After First Factor Authentication, the Customer needs to Register on Server and authenticate using Second Factor Authentication. This phase contains various Steps such as Login / Register / Verification / Password Change.

A. First Factor Authentication using Challenge Handshaking

If in Online Transaction Client want to communicate with Server, then first client sends a request to the server, the server responds. The server asks for the client to enter a challenge value. The server in respond to challenge value generates a master key using MD-5 hashing technique and responds client to enter his unique password. Since every client has its own password, so client enters his password and with the challenge value and password client calculates a master solution and respond back to the server. The server verifies both keys and authenticate client.

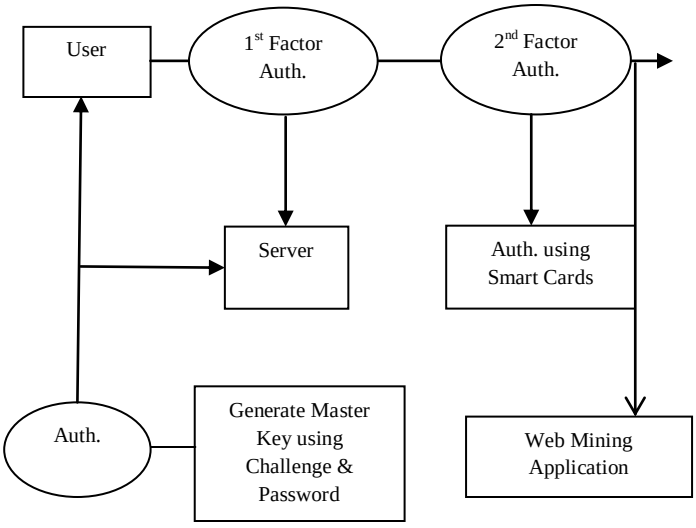


Fig 4 : A framework of Proposed methodology

Algorithm 1

1. First of all Customer will Sends request to the Server for the computed Challenge Value.
2. The Web Transaction Server will take the Challenge Value.
3. Server Computes Time Stamp T1.
4. Server will now take the Password value.
5. Server Sends Challenge Value with Time Stamp T1 to the Customer.
6. Customer then receivers the Challenge Value with Time Stamp T1 from the Server.
7. Customer then Computes Current Time Stamp T2.
8. On the basis of these Time Stamps T1 & T2, Customer calculates total transmission time.

$$Total_{transmission\ time} = 2 * (T2 - T1) + processing\ time$$

9. Customer now takes password and determine MD5 hashing function on challenge value + password +total transmission time.
10. Customer computes MD5 hashing on this data.
11. Customer will sends this data to Server.
12. Server received the data D1 from Customer and computes timestamp T3.
13. Server determines (challenge value + password + T3).
14. Server also determines MD5 hashing on (challenge value + password + T3).
15. If it matches then session is valid. Cheek whether the password valid or not
16. If valid send allowed else send not allowed else session expires.
17. Customer will show whether session expires or not.
18. If not expired then whether password valid or not.

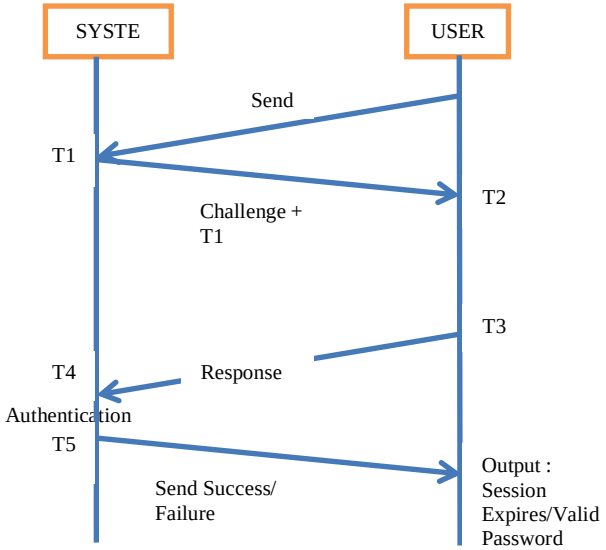


Fig 5: Architecture of the First Factor Authentication using Challenge Handshaking

B. Second Factor Authentication using Improved Smart Cards

The Second factor authentication involves use of Smart Cards for only one time Registration on the Server and Sending and receiving Transaction with high level Security with Asymmetric based Encryption.

The various Annotations used in the algorithms are as follows:

International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-8, Issue-3, May 2020
https://doi.org/10.21276/ijircst.2020.8.4.3
www.ijircst.org

Table 1: Various Annotations used in Algorithm

Customer / Client	U_i
Server	S
Customer ID	ID_i
Customer Password	PW_i
Hash(.)	One Way Hash function such as MD-5 / SHA-1 / SHA-256
$\|\|$	Concatenation
Xor	Xor operation
X	Secrete key of Server S
Tu	Transmission time
ΔT	Difference in transmission time

C. New Client Registration Segment

In the registering segment, client Ui requirements to record in inaccessible server S. Primarily client indicates his/her IDi and PWi. Previously catalogue on Server, recording consultant calculates hash (IDi) and hash (IDi||PWi) and guides to inaccessible server S over a secure frequency. The computed values are encrypted using characteristic based Encoding with Elliptical Curve based solution production and send to Server. Upon reception the registering claims from User Ui. Server Decrypts the Data using his Public Key and verifies the message. Server S analyzes same criticisms associated to the User Ui. S calculates

$$PA_i = Hash(ID_i).xor.hash(X_s||hash(ID_i))$$
$$PB_i = PA_i.xor.hash(ID_i||PW_i)$$
$$PC_i = hash(PA_i)$$
$$PD_i = hash(ID_i||PW_i).xor.hash(X_s)$$

And stowed a quantity in the elegant tag recollection and subjects this elegant certificate to Client Ui. This smart certificate is transported to Client Ui during a protected network.

a. Authentic Client Login Segment

This segment generates the capability of a protected entering to the client .client requirements to admission same services on distant server S. first it improvement the admittance correct on the isolated server S. Client Ui enters his smart certificate and enters his IDi* and PWi*. The reader calculates –

$$PA_i^* = PB_i.xor.hash(ID_i^*||PW_i^*)$$

And PCi* = hash (PAi*) and confirms whether PCi (which is generated in the elegant card reminiscence) and PCi* are comparable. If not, dismiss to over repetitive process. or else yes, Client Ui is a genuine possessor of the tidy certificate. On the other hand tag generates an arbitrary nonce Ri and calculates –

$$PE_i = PA_i^*.xor.PR_i$$
$$PC_{id} = hash(ID||PW).xor.PR_i$$
$$PF_i = hash(PA_i||PD_i||PR_i||T_u)$$

Where Tu is existing occasion when client entering request continue and propel the login demand knead {PFi, PEi, PCid, Tu, hash (IDi)} to inaccessible server S.

b. Confirmation/substantiation segment

Upon receiving the login application announcement {PFi, PEi, PCid, Tu, hash (IDi)}. Server authenticates the authority of time impediment between current (Tu') and previous time. Where Tu' is the journey period of the message/data. Current time (Tu')-previoud time (Tu) ≤ difference time (ΔT) where ΔT notates expect convincing time distance for communication impediment. Then server takes the entered appeal and go to subsequently progression, or else the server discard entered appeal.

Server calculates –

$$PA_i^* = hash(ID_i).xor.hash(X_s||hash(ID_i))$$
$$PR_i^* = PA_i^*.xor.PC_i$$
$$G = hash(ID_i||PW_i)^* = PC_{id}.xor.PR_i$$
$$PD_i^* = hash(ID_i||PW_i)^*.xor.hash(X_s)$$

And computes

$$PF^* = hash(PA_i^*||PD_i^*||PR_i^*||T_u)$$

And verifies to check PF and PF* are comparable. If not comparable then decline the entered appeal. If identical, then server S calculates–

PFs = hash (hash (IDi) || PDi || PRi || Ts) somewhere, current (Ts time) is isolated server in progress instance and throw recognize message {PFs, G, Ts} to user Ui. Upon receiving concede message smart card calculates

$$G^* = hash(ID_i||PW_i)$$
$$PF_s^* = hash(hash(ID_i)||PD_i||PR_i||T_s)$$

verifies that parameter (G) =G*and PFs = PFs* are identical or not with reciprocated substantiation progression. Here both Server and Client authenticate to each further. If they are identical then tag makes conference solution (Sk) and both Server and Client contribute to it.

$$S_k = hash(hash(ID_i)||T_s||T_u||PA_i$$

Otherwise dismiss to over entering progression.

c. Secret code modifies Phase

This stage is concerned every time Client U needs to modify the password (PW) with some more sophisticated Password (PWnew). Client U then enters his generated smart card and enters new (ID*) and new (PW*) and appeal to modify secret word. The tag then verifies parameter (C) = C* are comparable. If it is correct then Client U is a genuine owner of the tag. On the other hand tag asks the Client Ui to participate new code word PWnew. After inward bound the new secret word the tag calculate-

$B_{new} = PA_i.xor.hash(ID_i||PW_{new})$ and

$D_{new} = hash(ID_i||PW_{new}).xor.hash(ID_i||PW_i).xor.PD_i$

modify parameter (B) with Bnew and D with Dnew in smart tag memory.

IV. CONCLUSION

Security in various E-commerce Applications includes an efficient framework in Information Security especially in Data and Computer security and other IoT applications. Security in E-Commerce application plays an important role for the secure and scalable transaction which includes various dimensions such as security-integrity, Confidentiality, Non-repudiation, Privacy etc. Hence for the Security of Online Transactions in E-Commerce based application various Security algorithms are implemented. Although these Security algorithms are efficient and provides Security from attacks but Data Storage during the transactions and Computational time of the algorithms is also imperative. Hence an efficient algorithm is implemented which provides Security in Online E-Commerce transactions and also provides efficient Computational Cost and time.

The planned procedure implemented here works on the framework of Authentication on Two Factor which provides Security from attacks especially in IoT. The Methodology implemented works on two phases – in first phase assigning the validity of the User by allocating a challenge value and in second phase using improved smart card based authentication. The proposed technique prevents from numerous types of security attacks such as replay attack and identity disclosure attack or outsider attack and provides security from various dimensions such as security-integrity, Confidentiality, Non-repudiation, Privacy etc.

REFERENCES

[1] Xun Yi,"Security Analysis of Yang et al.'s Practical Password-Based Two-Server Authentication and Key Exchange System", 4th International Conference. Network and System Security (NSS), 2011.

[2] N. Kuruwitaarachchi, P.K.W. Abeygunawardena, L.Rupasingha & S.W.I.Udara, "A Systematic Review of Security in Electronic CommerceThreats and Frameworks", Global Journal of Computer Science and Technology: E Network, Web & Security Volume 19 Issue 1 Version 1.0, 2019.

[3] Haya Alshehri, Farid Meziane, "The Influence of Advanced and Secure E-Commerce Environments on Customers Behaviour: The Case of Saudis in the UK," in 12th International Conference for Internet Technology and Secured Transactions, 2017.

[4] Jiang Huiping. "Strong password authentication protocols",4th International Conference Distance Learning and Education (ICDLE),2010.

[5] Dr. Happy Agrawal, Moon Moon Lahiri, "Gender Influenced Online Shopping Behavior among College Students", Purakala (UGC Care Journal), Vol-31-Issue-55-June -2020

[6] J. Katz, R. Ostrovsky, and M. Yung: "Efficient And Secure Authenticated Key Exchange Using Weak Passwords". Journal of the ACM, 57(1):78–116, 2009.

[7] Shuo Zhai,"Design and implementation of password-based identity authentication system", 2010 International Conference Computer Application and System Modeling (ICCASM), 2010.

[8] Harold Nguegang Tewamba, Jean Robert Kala Kamdjoug, Georges Bell Bitjoka, Samuel Fosso Wamba, Nicolas Nkondock Mi Bahanag, "Effects of Information Security Management Systems on Firm Performance", American Journal of Operations Management and Information Systems, volume 4(3): pp. 99-108, 2019.

[9] S. Wanga, Z. Cao, K.-K. Choo, and L. Wang, "An improved identitybased key agreement protocol and its security proof," An International Journal of Information Sceinces, vol. 179, pp. 307-318, January. 2009.

[10] Puspa Indahati Sandhyaduhita, "Supporting and Inhibiting Factors of E-Commerce Adoption: Exploring the Sellers Side in Indonesia," in International Conference on Advanced Computer Science and Information Systems, 2016.

[11] D. XiaoFei and M. ChuanGui, "Cryptoanalysis and Improvements of Cross-Realm C2C PAKE Protocol,"WASE09, procedings of IEEE, International Conference on Information Engineering, pp. 193-196, 2009.

[12] Abdul Gaffar Khan, "Electronic Commerce: A Study on Benefits and Challeges in an Emerging Economy," Global Journal of Management and Business Research: B Economics and Commerce, vol. 16, no. 1, 2016

[13] Somdech Rungsrisawat, Thanaporn Sriyakul, Kittisak Jermsittiparsert, "The Era of e-Commerce & Online Marketing: Risks Associated with Online Shopping", International Journal of Innovation, Creativity and Change, Volume 8, Issue 8, 2019.

[14] Cong Cao, Jun Yan, Mengxiang Li, "The Effects of Consumer Perceived Different Service of Trusted Third Party on Trust Intention: An Empirical Study in Australia," in 14th IEEE International Conference on e-Business Engineering, 2017.

[15] Somdech Rungsrisawat, Watcharin Joemsittiprasert, Kittisak Jermsittiparsert, " Factors Determining Consumer Buying Behaviour in Online Shopping", International Journal of Innovation, Creativity and Change, Volume 8, Issue 8, 2019.

[16] Pu, Q.,"An improved two-factor authentication protocol". In: 2010 International Conference on Multimedia and Information Technology (MMIT). vol. 2, pp. 223– 226. Ieee, 2010.

[17] Xu, J., Zhu, W., Feng, D.:" An improved smart card based password authentication scheme with provable security". Computer Standards & Interfaces 31(4), 723–728, 2009.

[18] Abdullah, Madihah Mohd Saudi and Nor Badrul Anuar, "Mobile Botnet Detection: Proof of Concept", 2014 IEEE 5th Control and System Graduate Research Colloquium, 2014.

[19] Ghada El Haddad, Esma Aimeur, Hicham Hage, "Understanding Trust, Privacy and Financial Fears in Online Payment," in 17th IEEE International

Conference On Trust, Security And Privacy In Computing And Communications, 2018.

[20] "Trends in e-commerce & digital fraud: Mitigating the risks," EKN, 2017.

[21] Nik Alif Amri Nik Hashim et. al, "Internet Shopping: How the Consumer Purchase Behaviour is Impacted by Risk Perception", Test Engineering and Management, Published by: The Mattingley Publishing Co., Inc., Volume 59 Issue 6s Page Number: 1014- 1021, 2019.

SmallSEOTools

PLAGIARISM SCAN REPORT

Words	921	Date	August 15,2020
Characters	5994	Exclude Url	

0%	100%	0	41
Plagiarism	Unique	Plagiarized Sentences	Unique Sentences

Content Checked For Plagiarism

Chapter 1 Introduction 1.1 BACKGROUND What is online payment? Online payment, also known as electronic payment, it refers to the money which exchanged electronically. Broadly speaking, online payment refers to the transaction exchanged the funds on internet, typically involves computer network, internet and digital stored value system. It makes e-payment may at any time, via the internet directly to the transfer, settlement, and forms of e-commerce environment. How online payment basic process? Online payment may seem to be very easy and fast, but it consist of the confidential and security for the card info. In order to make sure that the process is work correctly, the merchant must connect to the network with the Issuing bank, processor, and others financial institution, so that the information that provided by the customer can be routed reliable and secure. As highly sensitive payment information, trust and confidence is an essential element of any payment transactions. This means that payment processing services should be provided by a wealth of experience in payment processing and security. What is electronic commerce? Electronic commerce refers to the goods and services which exchange over the internet, commonly known as e-commerce. All major retail organization also have an online presence, however, e-commerce also apply between business to business (B2B) transactions. It can open to all interested parties, or even limited participants. For example like Amazon.com, the selling and buying transaction is completed electronically and interactively in real-time. Besides that, e-commerce system also associated with the service industry, such as online banking, transfer funds, or even pay the credit card bill. 1.2 PROBLEM STATEMENT Security in various E-commerce Applications includes an efficient framework in Information Security especially in Computer security and Data Security and other Online transactions in E-commerce applications. Security in E-Commerce application plays an important role for the secure and scalable transaction which includes various dimensions such as security-integrity, Confidentiality, Non-repudiation, Privacy etc. Hence for the Security of Online Transactions in E-Commerce based application various Security algorithms are implemented. Although these Security algorithms are efficient and provides Security from various attacks but Data Storage during the transactions and Computational time of the algorithms is also important. • Security of e-commerce Along with the e-commerce continue to broaden, protection of individual treatment over the internet, and make your customers feel secure is the primary factors and necessary. In order to perform a secure and good service, internet security plays an important role to be enhancing in this situation. The objective is to establish rules and measure to use against attacks over the Internet. Internet information exchange on behalf of the invasion led to unsafe or high risk of fraud. For any expert in internet security will tell, e-commerce is actually much more secure than real world commerce. For example when you leave your credit card receipt in the shop, or accidentally give your credit card number to someone else, you are actually accepting the risk that the order which not order from you will appear on the next month's credit card bill. However, when you enter a credit card number of e-commerce site, you are sent through a secure connection to a server access only to authorized personnel and protected against even the most determined intruders. Although some of the people believe that transactions over the internet are in fact safer than offline transactions, there are still a number of people believe that offline transactions are always better than online payment. For example like protecting the credit card detail, company need to prevent the card info from customer or the privacy of the customer found by a third party. Typically, this involves the company network security and how the company provides a strong and secure system on the internet. 1.3 Common Online Payment System Online payment system is to help the consumer more convenience and it is the key issue to ensure that the consumer are fast and secure. There are several types of common online payment systems: • E-cash internet payment system E-cash, also known as electronic cash or electronic money, it is a form of data which exchanged electronically through the network computer or internet, these is electronic cash currency. It can be converted to cash value of the family of cryptographic sequences, and then use these sequences to show the value of all sizes. There are few characteristic are as follows: an agreement between the enterprises and banks and

the value of all sizes. There are few characteristic are as follows: an agreement between the enterprises and banks and authorization, can be transfer, can be kept, used to exchanged value within another system. As e-cash is what we can imagine as “cash” China’s purchase of small general merchandise payment habits features, it is likely to become an important means of online payment in China, but China has not officially started. There are many foreign companies to provide electronic cash market. If unconditionally anonymous electronic money digital cash net cash market can provide an anonymous e-money market. • E-purse Internet Payment System E-purse, also known as electronic purse, it is a type of smart card which embedded with the microchip. To use e-purse shopping, the first is the user must transfer certain amount of personal bank account, then in the corresponding of website to download electronic wallet service system free software and install an electronic wallet, to apply online and access the cardholder “electronic safety certificate. When users want to purchase something through the internet, just need to click on the “electronic wallet” icon, and follow the corresponding information that the user need to provided, such as password and user name to complete the transaction on the internet.

Sources	Similarity

SmallSEOTools

PLAGIARISM SCAN REPORT

Words	847	Date	August 15,2020
Characters	5303	Exclude Url	

9%	91%	3	32
Plagiarism	Unique	Plagiarized Sentences	Unique Sentences

Content Checked For Plagiarism

• Electronic check (E-check) Internet Payment System Electronic check, also known as e-check, is a form of payment which transfers through the internet. It performs the same function as the paper check of using digital transmission to transfer money from one account to one account. Besides that, e-check provide better security features than the paper check because it is an electronic format and may proceeded in fewer steps to complete the transaction. Most common features provided by electronic checks include authentication, public key cryptography, digital signatures or personal identification numbers instead of signature and so on. There's a simple electronic check process shown below: 1. Send Check Payee Payer 2. Inspect Check 3. Bill 4. Notice 5. Approve funds and transfer Payee Bank Accounting Server Electronic Check-Cashing Process E-check is an exclusive network system, the international financial institutions, with their equipment, software and hardware, an accurate and complete set if user identification, the standard messaging, data validation and other standardized data transmission agreement to make sure that the transaction are safety and security. • Digital Wallet Payment System A digital wallet, also known as e-wallet, it is a software system that store inside the user's computer to hold the digital cash, and a digital certificate with a digital signature. E-wallet allows users to make payment or transaction over the internet fast and safety. The function of the e-wallet is much more like a physical wallet, used to store the digital cash. After the e-cash service released, the e-wallet has evolved into a service to provide online shopping information and holds credit card data and passwords for logging into the website with a convenient way. An e-wallet have both software and information component. The software provides the safety and security with the encryption for the actual transaction. Typically, e-wallet is store on client side, so it is easier to self-maintenance and fully compatible with most of the online payment system. In addition, the system will automatically key in the user information in the online form, it is easier for the user and reduce the time to enter all the information again and again. While for the server side, it is refers to an organization and your side to create and maintain on it server. Because of the security and the efficiency and effectiveness of the utility that provided by the server-side to the users, it become more and more popular and famous for the user with the entire process. • PayPal System Listen PayPal is an e-commerce business by allowing the user to make transaction or money transfers through the Internet. PayPal also known as electronic alternative, such as checks and money are orders with the traditional paper method. It doesn't charge any fees to make any transaction or join the PayPal service, but they will be a fees change for those who want to receive the money from other people. PayPal account from a bank account can be funded by electronic debit or credit card. To receive the transaction from other people, the recipient from PayPal can either request from the PayPal service, established their own PayPal account, or request from their bank account. PayPal service is much like a intermediaries or a third party who involve between the clients and the recipient that facilitates in e-commerce. PayPal involve in several payments processing such as, online auction, online vendors, and others commercial users. It will cost some fees from the recipient for receiving money; fee included the percentage of the amount plus another additional amount. The fees is charged depend on the currency used, the option that choose by the user, the country of the sender and recipient (how far between both sender and recipient), the total amount sent by the sender and the type of account that the recipient receive it. In addition, shopping on eBay and then made the transaction by a credit card through PayPal may incur a "foreign transaction fee" if the seller is located in another country, as credit card issuers are automatically informed of the seller's country of origin. In my opinion, i strongly agree with the statement that the author mentioned about. Electronic cheque system provides several advantages than a paper based cheque such as faster speed transaction, provide a certain level of security like encryption or decryption, and so on. But there are still limits of disadvantages for electronic cheque system, like high fixed costs or development start-up costs. Besides that, electronic cheque system can be used in virtual world instead of the real world payment method. And the most important point is the security issue, because the less of face to face communication

world payment method. And the most important point is the security issue, because the less of face to face communication, we can't even know the actual user as well. The possibilities that someone is try to pretend as the actual user to make transaction with us and caused identity threat • Strength and Weakness • Advantages of Online Payment Online payment, what we called as online payment, is an indispensable business. This is extremely important to accept electronic payment of telecommunications service industry, because it started to use this rapidly growing economy is fully utilized.

Sources	Similarity
On-line Payment Sercurity | E Commerce | Online Safety & Privacy Electronic check system at present is an exclusive network system, the international financial institutions, through their own private networks, equipment, software and a complete set of user identification, the standard messaging, data validation and other standardized data transmission... https://www.scribd.com/document/86918871/On-line-Payment-Sercurity	10%
Online Payment Methods for Indian Bettors - BET-INDIA the function of the e-wallet is much more like a physical wallet, used to store the digital cash. after the e-cash service released, the e-wallet has evolved into service to provide online shopping information and holds credit card data and passwords for logging into the website in a convenient way. https://bet-india.com/online-payment-methods/	10%
Cartaspedia: Paypal in addition, ebay purchases made by credit card through paypal may incur a "foreign transaction fee" if the seller is located in another country, as credit card issuers are automatically informed of the seller's country of origin. on october 3, 2002, paypal became a wholly owned subsidiary of ebay. http://cartaspedia.blogspot.com/2009/11/paypal.html	4%

SmallSEOTools

PLAGIARISM SCAN REPORT

Words	925	Date	August 15,2020
Characters	5561	Exclude Url	

0%	100%	0	39
Plagiarism	Unique	Plagiarized Sentences	Unique Sentences

Content Checked For Plagiarism

1.4 There are several advantages of online payment (e-payment): • Convenient and 24 hour's real time transaction Through the use of online payment system, consumer can access the web to make any transaction such as online banking, online billing or even car loan at any time (24 hours) or anywhere, as long as access to the internet. For example like consumer can check the bank details through their mobile phone no matter at where and anytime along with the network connection. In addition, consumer able to check or view the history of the previous transaction that they made or get the accurate real time information through online payment system. It may save up a lot of the paperwork as well. • Reduce cost and save time With the help of online payment system, we only need to stay at home with just a click in front of the computer which connected to the network, and transaction will be done easily. Instead of go to the physical bank to make the transaction by writing the form and waiting in front of the counter. It may save up a lot of cost like transportation fees, paper workflow fees and so on. Besides that, through online payment, the processing speed is definitely fast and rapid by following the simple instructions and entering the parameters that the system required. And user may not need to transport from one location to another, it may save up a lot of time. Compared with the real world physical offline banking system, it may spend a lot of time especially on peak season or peak hour. • Flexible of using e-payment Along with the continuous improvement of e-commerce, many organizations or firms not only focusing their business on offline operation, but managing their business workflow on internet. Nevertheless, e-payment, as what we called as online payment, had become an indispensable item for the entire progress of e-business. Nowadays, there are more and more online payment service provided which linked with the organization. It is more flexible to the consumer, they can choose which type of service that they want, for example like PayPal, e-cash or which bank they prefer such as maybank2u and so on. Besides that, majority of the online payment service are operation 24 hours, consumer can make the transaction anytime they like. In addition, they can reduce they pain of transport from one location to another and waiting in-front of the counter in the bank. Online payment service allow consumer to make any transaction on anytime or everywhere by accessing to the network. It is the flexibility of e-payment. • Benefit between consumer and organization With the help of online payment, consumer and organization are benefiting in other ways like the consumer and organization are able to negotiate arrangements for the true value, and strengthen the relationship of their business. Besides that, consumer can skip many steps or documentation for the transaction. It may easier for them to control over the timing of payment steps, and minimize the operation of the idle account balance. Consumer can eliminate the delay for the processing of transaction. For organization, they can reduce the cost of processing the paper cheque. Yet when the organizations process the paper cheque that paid from consumers, they need to spend some cost to process the paper cheque. With the help of online payment, the organization may have the advantages as well by encouraging the consumer to pay electronically instead of pay by a paper cheque. In addition, they can receive the payment immediately without any delay, because the receipt is available immediately after consumer had made the payment. • Others common benefits Below are some of the common benefits for online payment method. Personal security We do not need to hold so much money along with us on our premises, or even on the outside, and lead to more safety and security. Used internationally Online payment is a common method that can be used internationally, it is important for the tourist-sector businesses or those organization who running their business or selling their goods overseas. Reaching a wider customer base Some of the organizations accept the online payment method like phone delivery or mail ordering for online customers; it is easier for those customers who are lack of transportation or not able to reach your premises. Increase the sale opportunities For some customer willing to buy the goods from the offline business shop, the may having the problem that insufficient fund, they have to leaves to get cash, it may cause them not return to the shop again. With the help of online payment from ecommerce sector, customer can buy the goods from internet as long as the computer or devices are connected to the internet. This may lead to sale increasing

the goods from internet as long as the computer or devices are connected to the internet. This may lead to sale increasing. 1.5 Disadvantages of Online Payment The transaction over the internet or the transfer of fund on internet through the electronic media is known as electronic payment, as what we called as online payment. Nowadays, online payment is a daily activity for most of the business organization. It is very common and convenient for the online transaction for those organizations focus their business over web to interact with their consumers or business partners. In fact, there are still weaknesses of the online payment that we cannot ignore it. One of the ways is to be aware the raised awareness of privacy and security issues from the electronic online payment system. Consumers have to bear the risk such as fraud or identity threat that involved in the online transaction.

Sources	Similarity

SmallSEOTools

PLAGIARISM SCAN REPORT

Words	944	Date	August 15,2020
Characters	5776	Exclude Url	

7%	93%	3	40
Plagiarism	Unique	Plagiarized Sentences	Unique Sentences

Content Checked For Plagiarism

There are several disadvantages of online payment (e-payment): • Privacy security concerns. In the e-commerce world, most of the online banking systems, also known as online transaction site, require the user to register as their own member with some simple input or instruction before giving the authorization for them to make the transaction. While the registration process, user need to provide the username and password, all these information implies the need of privacy protection and security. In addition, user need to maintain their account, it may be a trouble for the user. For those organizations' site that hosting the user account, they should follow the strict of security and privacy policies. It is very important for those organizations to protect the privacy of the user details and prevent the information being hacked by the hacker. If the username or password is susceptible to being hacked, it maybe will cause the user a serious financial loss problem from the end. All these are a potential rick of the privacy or the personal detail being hacked while using the online payment system. • Identity theft Another disadvantage of using online payment is identity theft. Using the right security measure can prevent your important information being exposed by the third party. Besides that, using virus protection or firewall may very useful to protect your computer. It might a risk that you make any transaction through internet from your computer. Another example like if you losing your smart card, unfortunately the card is fall in unsafe of person's hand. There is a very serious or dangerous expenditure of your entire account balance. Though you will inform the authorities on card's loss, when the time between you losing your card and informing to the authorities, the third party (unsafe person) may transfer all your money out through your card details via internet. • Dependency of online payment system Along with the information technology, many organizations or firms are running their business over the internet and provide several utilities as long as online transaction. In fact, this method is indirectly effect consumers become more and more dependent on online transaction, because it speed and rapid transaction, availability 24 hours as long as connected to the internet at home or even a mobile devices. However, there still can be disadvantages for over dependent of online transaction. For example like if the email does not send to the right destination or not working well, the sender may not know the sending error or does the email has reach the destination or not. Or like for those consumers may want to pay the bill or loan over the internet instead of the traditional ways. There might be a possibility that the online payment system down or not function well from the server side, and worst there was a way for the consumer to meet the dead line. • Loss human touch In the physical bank, some of the customer may like to talk and communicate with the bank tellers, interacting with the bank manager or even the bank clients. But in the online virtual world, online banking system had taken off of these "human interactions"; all these are done by a system program, impersonal hand-off process. Due to the lack of the "human interaction" for online payment system, some of the customer my not know about the knowledge of online payment system. These required a basic computer skill and the knowledge about internet before using the online payment system. In addition, for some of the small online banking system, they may not provide any instruction or any guideline to lead the user in the correct way. It will cause the users entering the wrong information or incorrect bank details through the online payment system. • High cost development for internet payment gateway The major disadvantage for online payment method is the high cost for internet payment gateway. For those organizations or firms are running their business over the internet, the have to create an internet payment gateway or a system in-house is definitely high development cost. For those non IT companies, it is hard and difficult for them to create a system for their own. Because it wasn't their core business, and they had to use the resource from inside the company with a little or even zero of IT knowledge to build it up. Therefore, the company have to outsource from outside to help them develop a new online payment gateway for them. • Others Limitation Others common limitation of the online payment method: May be difficult to inspect from a remote location Limited of countries cultural and legal obstacles The rapid changing of technologies Hard to retaining the employee Government regulators Difficult to integrate the software of transaction process and the

Hard to retaining the employee Government regulators Difficult to integrate the software of transaction process and the current existing database. Critical Evaluation Based on Olga Lu et.al (2009, p.15-16) The main benefit from the bank customers' point of view is significant saving of time by the automation of banking services processing and introduction of an easy maintenance tools for managing customer's money. Private customers seek slightly different kind of benefits from e-banking. In the study on online banking drivers Aladwani (2001) has found, that providing faster, easier and more reliable services to customers were amongst the top drivers of e-banking development. In my opinion, I definitely agree with the above statement that stated by author (Olga Lu et. al). Online payment may help to reduce costs and convenience; user may stay at home to performed transaction at any time as long as connected with the network. It is fast and provides funds management, which allow user to download the history of the transaction that that had made.

Sources	Similarity
Introduction and Statement of Problem (customer-oriented system). the most important distinction of this period is that banks are planning to release employees who are working insaving of time by the automation of e-banking services, processing, and the introduction of an easy maintenance tools for managing customer"s money. https://shodhganga.inflibnet.ac.in/bitstream/10603/28610/9/09_chapter 1.pdf	3%
E Banking Benefits | Online Banking | Monetary Policy 4) private customers seek slightly different kind of benefits from e-banking.customers can download their history of different accounts and do a what-if services. from the place a customer wants to. minute before concluding a fund transfer. analysis on their own pc before affecting any transaction... https://www.scribd.com/document/148489817/E-Banking-Benefits	3%
Lust Sik | Online Banking | Debit Card as online internet banking and mobile phone banking are the most quickly developing areas, in the present paper the focus is mainly on thein the study on online banking drivers aladwani (2001) has found, that providing faster, easier and more reliable services to customers were amongst... https://www.scribd.com/document/133094606/Lust-Sik	3%

SmallSEOTools

PLAGIARISM SCAN REPORT

Words	989	Date	August 15,2020
Characters	6318	Exclude Url	

12%	88%	6	44
Plagiarism	Unique	Plagiarized Sentences	Unique Sentences

Content Checked For Plagiarism

1.8 Strategic of E-commerce Security As e-commerce security cause by many factors such as fraud, identity theft, or confidential data being steal by the hacker, all these are the problem that we might face it when in the online virtual world. So, a strategic planning for ecommerce is very important, all the strategic that came out should be line with the overall of the ecommerce business management. It must provide a very powerful protection for all the ecommerce confidential data and allow them to recover as fast as possible if any incident happen. To prevent the security problem happen, a set of variety measurement must be included. 1.8.1 Security Strategy In order to ensure secure communications between both parties on internet, we must take the necessary measures to prevent them. For communication link purpose, we can use firewall or Virtual Private Network (VPN) to make the communication more safety and secure. And consumer must be very careful on some of the untrusted Proxy server. It is act like an intermediary for seeking the information, resource, or link that requested by the client. If the consumer are using the untrusted proxy server, all the data that the client provided may not be encrypted and sent to the proxy server, and proxy server may record down everything sent from the client, including the login and password. For identification and authentication purpose, encrypted or hash function may be very useful in this situation. In ecommerce, login is a very common and the first step for the consumer before they move on the transaction step. To login to the system, the system needs to identify the user name and password before provide the authentication to the user. With the help of encryption, user password have more secure which showing the password in "*" symbol. In order to provide security to the customer, existing banking system uses various level of security mechanisms. Even though tough encryption standards are provided against network attacks, it is prone to be broken. Intruders are smart enough to retrieve the passwords of the customers through online transaction. As per the world payments report, in current technology people prefer to use cashless payments rather than the cheques or cash payments. As we all know that these kinds of e-transactions provide huge number of benefits to the customers for example, by making the transactions easier, faster and instant payments. As per the survey an Indian uses online transaction system once in a week for payment. This online transaction might be through credit/debit cards, e-wallets, UPI's, food cards, travel cards and some authorized e-payment systems. Many security implementation methods like hardware level security, antivirus, anti- malware and antispyware programs, strong passwords, single time bound OTP system, virtual private network, secured site uses SSL certificate are used in practice. However, in spite of all these security mechanisms intruders go for brute force attempts to decrypt the PIN numbers and passwords etc. So, single level encryption standard is not sufficient to provide high level security for online transaction system. At present we need to have a multilevel encryption standard wherein even if anyone encryption standard is broken, the online transaction requested by the customer will be completed with the other encryption standard. Our paper focuses on multilevel security with Blowfish and AES algorithm along with dual OTP scheme which may lead to stronger level of protection against threat encountered in online transactions. E-Commerce refers to the activity of buying and selling things over the internet. Simply, it refers to the commercial transactions which are conducted online. E-commerce can be drawn on many technologies such as mobile commerce, Internet marketing, online transaction processing, electronic funds transfer, supply chain management, electronic data interchange (EDI), inventory management systems, and automated data collection systems. E-commerce threat is occurring by using the internet for unfair means with the intention of stealing, fraud and security breach. There are various types of e-commerce threats. Some are accidental, some are purposeful, and some of them are due to human error. The most common security threats are an electronic payments system, e-cash, data misuse, credit/debit card frauds, etc. 1.9 Electronic payments system: With the rapid development of the computer, mobile, and network technology, e-commerce has become a routine part of human life. In e-commerce, the customer can order products at home and save time for doing other things. There is no need of visiting a store or a shop. The customer can select different stores on the Internet in a very short

things. There is no need of visiting a store or a shop. The customer can select different stores on the internet in a very short time and compare the products with different characteristics such as price, colour, and quality. The electronic payment systems have a very important role in e-commerce. E-commerce organizations use electronic payment systems that refer to paperless monetary transactions. It revolutionized the business processing by reducing paperwork, transaction costs, and labour cost. E-commerce processing is user-friendly and less time consuming than manual processing. Electronic commerce helps a business organization expand its market reach expansion. There is a certain risk with the electronic payments system. 1.9.1 Some of them are: • The Risk of Fraud An electronic payment system has a huge risk of fraud. The computing devices use an identity of the person for authorizing a payment such as passwords and security questions. These authentications are not full proof in determining the identity of a person. If the password and the answers to the security questions are matched, the system doesn't care who is on the other side. If someone has access to our password or the answers to our security question, he will gain access to our money and can steal it from us. • The Risk of Tax Evasion The Internal Revenue Service law requires that every business declare their financial transactions and provide paper records so that tax compliance can be verified. The problem with electronic systems is that they don't provide cleanly into this paradigm. It makes the process of tax collection very frustrating for the Internal Revenue Service.

Sources	Similarity
e Commerce | E Commerce | Automated Teller Machine e-commerce refers to the activity of buying and selling things over the internet. simply, it refers to the commercial transactions which are conducted online. e-commerce can be drawn on many technologies such as mobile commerce, internet marketing, online transaction processing, electronic... https://www.scribd.com/document/436600816/e-Commerce	10%
what are the security threads for e commerce system - Brainly.in some are accidental, some are purposeful, and some of them are due to human error. the most security threats are pishing attacks, money theft, data misuse, hicking, credit card fraud, and unprotected services. inaccurate management-one of the main reasons for... https://brainly.in/question/12472399	3%
Analysis on online payment systems of e-commerce e-commerce enterprises use online payment systems that refer to paperless monetary transactions, which has revolutionized the business processingbeing user-friendly and less time consuming than manual processing, electronic commerce helps a business organization expand its market reach... https://www.theseus.fi/bitstream/handle/10024/139600/Yang_Wenjing.pdf?sequence=1&isAllowed=y	2%

SmallSEOTools

PLAGIARISM SCAN REPORT

Words	391	Date	August 15,2020
Characters	2957	Exclude Url	

14%	86%	3	18
Plagiarism	Unique	Plagiarized Sentences	Unique Sentences

Content Checked For Plagiarism

1.10 Why you can't afford to overlook e Commerce security? While growth in e Commerce has improved online transactions, it has attracted the attention of the bad players in equal measures. E Commerce cybercrime reports reveal that the industry is among the most vulnerable ones when it comes to cybercrimes. The e Commerce world experiences about 32.4% of all attacks. 50% of small e Commerce store owners are lamenting that the attacks are becoming severe. Furthermore, the reports show that 29% of traffic accessing a website consists of malicious requests. Such attacks have contributed to significant losses in financials, market shares, and reputation. Almost 60% of small e Commerce stores that experience cybercrimes don't survive more than six months. Therefore, it is very crucial to put in place water-tight security measures and hire a robust team. It will ensure you run your business without worrying about closing down due to cybercriminals. 1.11 SECURE THIRD PARTY AUDITING FRAMEWORK Secure Third Party Auditing agenda and crucial workings of the haze figuring situation are shown in Character. The TPA Auditing Manager enables partnership amongst dissimilar provision wage-earners by constituting new necessary amenities. Respectively TPA Auditing Manager has machineries that are answerable for formation and conservation of conviction amongst the indigenous worker spheres and amongst the wage-earners and the operators, provisioning necessary amenities and producing worldwide strategies. The provision integrators initial determine amenities from dissimilar provision wage-earners or additional TPA Reviewing Director transport out discussions, assimilate the amenities to method collections of cooperating amenities and deliver them to manipulators. The refuge administration constituent delivers the sanctuary and confidentiality description and application functionality. The confirmation and uniqueness administration component is accountable for confirming employers and amenities grounded on authorizations and features. In provision wage-earner, the admittance regulator component employments the admittance strategies while the discretion and statistics encryption component is answerable for confidentiality requirements and encryption of subcontracted statistics. In the provision integrator, the conviction founded strategy incorporation component is the significant constituent that manages conviction and enables conviction grounded strategy combination between dissimilar amenities from dissimilar provision benefactors. The provision administration constituent is answerable for protected provision unearthing, configuration and provisioning. The package benefactor customs virtualization in command to suggestion amenities to employers are more competently. The provision unearthing component is answerable for conclusion dissimilar amenities that the benefactor provinces or other provision integrators proposition.

Sources	Similarity
Ecommerce Security: Importance, Issues & Protection Measures furthermore, the reports show that 29% of traffic accessing a website consists of malicious requests. such attacks have contributed to significant losses in financials, market shares, and reputation. almost 60% of small ecommerce stores that experience cybercrimes don't survive more... https://www.getastra.com/blog/knowledge-base/ecommerce-security/	30%

SmallSEOTools

PLAGIARISM SCAN REPORT

Words	982	Date	August 15,2020
Characters	6788	Exclude Url	

0%	100%	0	6
Plagiarism	Unique	Plagiarized Sentences	Unique Sentences

Content Checked For Plagiarism

Chapter 2 LITERATURE SURVEY 2.1 PASSWORD BASED TWO SERVER AUTHENTICATION SYSTEM Present Works: Here is so countless identification obtainable about this two waitron confirmation organization. The planned organizations are Biometric based impression confirmation, key argument based confirmation and watchword lone with no significant conversation etiquette type etc. Zung Yang who confirmed the concept of a “Real-world Watchword Grounded Confirmation Organization for Key Discussion”, the only aberrant with that concept is the comfort of assumed. Even nonetheless that is definite, that is not an easy occupation for a beginner user to comprehend. Subsequently the second hand so many multilayered connotations by proceeds of encryption and cunning, which are challenging to understand as glowing to apparatus also. Registration stage: In the registering phase, the manipulator has to arrive the watchword and additional one accidental quantity which would be at smallest two less than the distance of the watchword. (i.e.) 1

Sources	Similarity

SmallSEOTools

PLAGIARISM SCAN REPORT

Words	819	Date	August 15,2020
Characters	5596	Exclude Url	

0%	100%	0	35
Plagiarism	Unique	Plagiarized Sentences	Unique Sentences

Content Checked For Plagiarism

2.4.1 Key Privacy Unique conceivable trouble of a 3-party flawless is that the discretion of the announcement with approbation to the waitperson is not continuously convinced. Since we poverty to confidence as diminutive as believable the third get-together, we developed a new interpretation named key confidentiality which tastelessly incomes that, even however the waitron's help is obligatory to generate an assembly key among two employers in the procedure, the waitron should be intelligent to upsurge any substantial on the charge of that meeting important. Here we commence that the waitron is dependable but curious. Gratify message that crucial circulation provisions frequently do not realize this stuff. 2.4.2 Insider Attacks One of the chief alterations amongst the 2 revelry and the 3 revelry states is the company of insider sessions. To improved appreciate the control of these quantities, thoughtful the propriety in Numeral 1, grounded on the coded key disagreement of, in which the waitron merely decodes the communication it accepts and re-encrypts it underneath the supplementary employer's watchword. In this custom, it is familiar to see that unique can attitude an off-line vocabulary by merely singing the character of one of the complicated gatherings. Announcement that both A and B can achieve. 2.4.3 A New Security Model In command to examine the refuge of 3 revelry watchword grounded dependable important conversation manners, we put progressing a new-fangled shelter conventional and designate two notions of sanctuary: in distinguish ability of the assembly significant and important discretion with admiration to the waitperson. The original of these philosophies is the usual one and is a traditional advancing simplification of the communicator thought in the 2-party watchword grounded dependable key argument conventional. The another one is new-fangled and accurate to the new condition, and confinements the concealment of the significant with reverence to the imperative waitron to which all keywords are acknowledged. 2.4.4 The Need for New Security Notions Astonishingly, the unaffected of protection for the original fangled organization prepares not appear to gumshoe from the distinctive sanctuary thoughts for the important organizations as one would supposing and seems to dictate a new-fangled and tougher concept of protection for the important 2 get-together watchword founded procedure (see Segment 2). In circumstance, this newfangled refuge thought is not exact to watchword grounded provisions and is one of the foremost charities of this newspaper. Conveniently, we distinguish that most contemporary 2-party watchword grounded provisions do in condition delight this new material. More exactly, only a few unimportant disparities are obligatory in their water-resistant. The EKE technique documents two communication articles to authorize each supplementary and to generate an inactive key for stimulating advanced programmers via a feeble keyword. Subsequently then, frequent two-party watchword founded genuine key founding measures have been intentional to improvement sanctuary and demonstration. These arrangements deliberate confirmation amongst a shopper and a waitperson and undertake that the two complex substances are consumer and waitron congruently and they portion a mutual watchword. With assortment and expansion of communiqué surroundings in the grounds such as mobile systems, home schmoozing and etc., these categories of communiqué systems propose to assimilate into the Internet and the end to-end sanctuary is painstaking as one of the significant questions in deceitful next cohort Internet know-how. To dodge this inconvenience, some of intentional PAKE etiquettes are prolonged to take into explanation the 3-partysituation, in which an important waitperson happens to intercede among two statement assemblies to document shared corroboration. Such actions only demand that each statement article dividends a keyword with an important waitron. Though, in achieves, they

are fewer unhurried in an irritated monarchy place like in Kerberos organization. In an irritable monarchy position, two clienteles are in two dissimilar Kerberos dominions and hence forth double waitrons (which are associated with a symmetric crucial) are compound. Some instructors, e.g.do not contemplate it compulsory to contemplate that situation since they have assumed that all waitrons in the universal instance know all manipulators' watchwords. Really, in the measures with a irritable realm backcloth, it is substantial to antitude that one attendant ought not find the keyword of a shopper in supplementary

realm backcloth, it is substantial to aptitude that one attendant ought not find the keyword of a shopper in supplementary dominion. 2.4.5 Protocol Syntax Etiquette Contributors: The dispersed organization we reflect is completed up of three separate crowds: S, the set of reliable waitrons; C, the customary of authentic patrons; and E, the customary of malevolent patrons. We also represent the customary of all regulars by U. That is, U = C [E. In an irritable monarchy setting, we undertake S to comprise two important waitpersons. The enclosure of the malevolent set E between the contributors is one the core variances amongst the2-party and the multi-party representations. Such addition is wanted in the multi-party standard in knowledge to accomplish with the likelihood of insider occurrences. The customary of spiteful operators prepared not necessity to be measured in the 2gathering due to the individuality between the keywords communal amongst couples of authentic contributors and persons communal with spiteful operators.

Sources	Similarity

SmallSEOTools

PLAGIARISM SCAN REPORT

Words	921	Date	August 15,2020
Characters	6476	Exclude Url	

0%	100%	0	43
Plagiarism	Unique	Plagiarized Sentences	Unique Sentences

Content Checked For Plagiarism

2.5 THE SECURITY MODEL The communication amongst a challenger A and the etiquette contributors happens only via oracle enquiries, which classical the challenger competences in a physical attack. In the occurrence, each of procedure contributors may have numerous incidences baptized oracles compound in dissimilar, maybe harmonized, performances of the etiquette. We represent the U's i-th (resp. S's j-th) occurrence by Ui(resp. Sj). The categories of oracles accessible to the challenger are as shadows: ²Execute (Ui11 ; Sj11 ; Sj22 ;Ui22)This question representation sun receptive occurrences in which the aggressor overhears on truthful performances between the customer occurrences Ui11 andUi22 and important waiter occurrences Sj11 and Sj22 . The productivity of this inquiry comprises of the transportations that were substituted through the truthful operation of the etiquette. Send Consumer (Ui;m): This question symbols an dynamic occurrence, where the contender may disturb a memorandum and formerly regulate it, generate a new-fangled one, or merely continuing it to the intended shopper. The production of this inquiry is the memorandum that shopper occurrence Ui would harvest upon reaction of communication m. Send Server (Sj; m):This enquiry mockup a vigorous bout alongside a waitron. It productivities the communication that waitron occurrence Sj would produce upon receiving of memorandum m. Reveal (Ui): This enquiry mockup the misapplication of sitting answers by customers. If a sitting crucial is not distinct for occurrence Ui, then reoccurrence? Then, reoccurrence the assembly key apprehended by the incidence Ui. Test (Ui): This inquiry is used to incarceration the contestant's skill to tell apart a corporeal desk bound important from an unintended one. In knowledge to account it, we primary casual a(private) coin b and then progressing to the opponent moreover the sitting key sk apprehended by Ui(i.e., the charge that a enquiry Reveal(Ui) would production) if b = 1 or a accidental important of the identical size if b =0. 2.5.1 Strengthening Passwords The expediency of user preferred watchword confirmation etiquettes has instigated them to be extensively positioned. Between the feebler etiquettes unique discoveries watchwords directed in the strong, returnable squat entropy PINs, and confusion based contest answer practices. A normally secondhand, and improved, method is to guide a watchword or watchword hash over a wait person side SSL- authentic assembly. Theoretically, these methods still agonize from the detail that a user may be deceived into see-through his watchword to a waitron who does not distinguish it. The assistances of a zero-knowledge grounded method were comprehended. The objective of such conventions is to deliver a confirmation technique which does not divulge an employer watchword to any get-together who does not previously have it. This streak of investigation constant in numerous instructions and characterize a noteworthy development in client waiter conventions. Watchwords continue the most prevalent technique of user confirmation to date, not withstanding their characteristic faintness. For instance, user watchwords, or watchword misunderstandings are recurrently packed in a server folder, and the user confirms by distribution the keyword backbone using a server-side SSL reliable system. Of development, all watchword organizations document an aggressor to brand some quantity of deductions before the wait person tresses the interpretation depressed. Though, a much additional thoughtful weakness occurs: in case of a waitperson negotiation, an aggressor may acquire all user watchwords, or watchword confusions in the folder at once. Manifold Waitperson Use: Notwithstanding the enhancements labeled above, solitary server watchword grounded confirmation etiquettes do not defend from waitperson cooperation in an acceptable way. Characteristically, an assailant who openings a server will be cheerful to improvement a very inordinate number of user watchwords; possibly after consecutively a vocabulary spell (salt only decelerates this). The normal method to lecturing this weakness is the use of manifold waitpersons. In such provisions, the capability of demonstrating a keyword is divided amongst two or more gadgets, and more than an influenced brink number of waitpersons requirement to collaborate to recuperate the watchword. 2.5.2 Verifiable Security Progressively, it has been comprehended that the application of a cryptographic arrangement is only as appreciated as its supplementary demonstrable refuge examination. The refuge proof systems based on intricacy hypothetical practicalities

supplementary demonstrable refuge examination. The refuge proof systems based on intricacy hypothetical practicalities, counting the abundant all-purpose consequences on protected multi-party calculation and beginning cryptography, deliver tackles for examining the classes of etiquettes we are attentive in. Characteristically, this outline is used to contemporary a symptotic sanctuary descriptions and sanctuary testimonies. Nevertheless, for a procedure which is to be organized, an existing refuge investigation is mandatory. 2.5.3 Communication Framework and Desired Security A binary waitron confirmation procedure contains a Consumer and two waitrons. Subsequent, the binary waitrons determination be signified Blue and Red. Throughout a matriculation opinion, the operator indicates a watchword, which is handled by the customer to harvest registering communications for each waitron. Advanced, once an applicant arrives a watchword, the customer concocts and directs confirmation communications to each waitron. Afterward the dual waitrons comprehensive a corroboration etiquette, the applicant is informed of the consequence by unique o rtogether waitrons. To traditional a condition in which the characteristics of the Blue and Red waitrons are effortlessly established, we shoulder that all get-togethers employment a protected network to Blue and Red. In repetition, this can be comprehended with SSL. Architecturally, it might be desirable for the purchaser to connect with a solitary waitron, and this is naturally brilliant by discussing one waitperson (say Blue) as a router. The booklover will effortlessly authenticate that the etiquettes we designate are comprehensive; a plaintiff with accurate watchword will continually confirm appropriately. More hard is to demonstration the unassailability stuff: that a challenger cannot do considerable improved than watchword fathoming.

Sources	Similarity

SmallSEOTools

PLAGIARISM SCAN REPORT

Words	999	Date	August 15,2020
Characters	7388	Exclude Url	

0%	100%	0	43
Plagiarism	Unique	Plagiarized Sentences	Unique Sentences

Content Checked For Plagiarism

2.5.4 Limitations of the Model For thickness, customary the quarrelsome area to be reassurance the non dishonored waitron to validate the opponent as operator username. It is straightforward to change the scrupulous hearings considered underneath for the line of suitably predicting the watchword. This container be a supplementary normal goal, for example, once one waitron (Blue) is surrendering admittance to approximately provision, and additional(Red) is contemporary to eradicate a solitary opinion of watchword cooperation. Formerly, the normal goalmouth of an opponent bargaining Blue is to absorb user watchwords. The confrontational competences designated overhead do not amount the possible benefit an opponent strength improvement from inputting mistake. Subsequently the adversary is sonly allowable to generate the purchaser on the accurate watchword, the prototypical does not imprisonment the probable benefit for an opponent who detects a customer introduction the confirmation arrangement with an inappropriate but associated watchword. Though it is maladroit to prototypical, it is believable that a challenger strength assistance from this. 2.6 SMART CARD AUTHENTICATION Watchword verification with clever card is unique of the maximum convenient and actual two influence authorization gadgets for isolated administrations to assurance one cooperating get-together of the fairness of the dependable festivity by acquisition of corroborative indication. This technique has been extensively located for frequent varieties of authorization requirements, such as inaccessible congregation login, connected investment, e-commerce and e-health [19]. In totaling, it establishes the foundation of three influence confirmation [20]. However, here still ensues courts-martial in both sanctuary and performance landscapes unpaid to the stringent refuge provisions and replacement stressed topographies of the customers. Presented the first unfriendly operator authorization preparation using shrewd cards there have been numerous of such provisions deliberate [21, 22, 23, 24, 25, 26, 27]. In 2010, Pu [27] piercing out Yang et al.'s arrangement is susceptible to important negotiation occurrence. Astonishingly, we originate Yang et al.'s outline motionless cannot accomplish its demanded foremost sanctuary goalmouth by representative a disconnected watchword predicting occurrence in Supplement A, and finished the refuge investigation of Yang et al.'s arrangement, some delicacies and contests in conniving this type of arrangements, dissimilar from the outdated watchword grounded confirmation, are exposed. Subsequent Yang et al.'s influential exertion, many heightened systems [28] have been intentional to dissertation the canny card protection introductory aberrant, nonetheless, maximum of them were currently originate partaking frequent sanctuary indistinctness actuality unnoticed [29, 30] Curiously, unfluctuating have been delivered with a prescribed proof. 2.7 ADVERSARY MODEL AND EVALUATION CRITERIA Nearby have remained numerous identifications commerce with shrewd card-based keyword corroboration preparations in current centuries (see, e.g., [30]). Though, in maximum of these educations, the novelists present-day occurrences on earlier arrangements and recommend new-fangled procedures with proclamations of the greater characteristics of their arrangements, while disregarding assistances that their arrangement doesn't effort (or bomb) to deliver, thus overseeing scopes on which it charges unwell. Notwithstanding the nonexistence of assessment standards, additional common artefact of these instructions is that, around is no appropriate refuge explanation (or smooth an obvious refuge classical) accessible. Therefore, in the subsequent, an challenger classical dependable with the genuineness is clearly demarcated and a all-inclusive measures set is projected. 2.7.1 Adversary Model In the predictable watchword authentic key argument conventions, the aggressor is demonstrated to have the occupied regulator of the announcement network amongst the collaborating get-togethers, such as snooping, stopping, implanting, removing, and adjusting any communicated communications over the communal network. Nevertheless, this supposition is sensible for password-based confirmation circumstances, it is not adequate for watchword based distant confirmation using smartcards. Current edifications have exposed that the underground information in the smart card might be uninvolved out by checking influence ingesting or retaining contrary business methods. Therefore, the escape of subtles structures deposited in the smart card may principal

retaining contrary business methods. Therefore, the escape of subtles structures deposited in the smart card may principal the unique protected arrangements weak to smart card damage problematic, such as disconnected keyword cracking occurrence and impression occurrence. Furthermore, as experimental and in-deep explored by Wang rather newly, spiteful card students also pay to the refuge disappointments of such arrangements. When the card student is underneath the regulator of the assailant, the smart card proprietor's contribution watchword may be interrupted (but the underground material deposited in the card would not be exposed at the same period, the modest motive is that an aggressor cannot recited the delicate material on the card within adiminutive time dated). However, we confine the aggressor from first stopping the watchword via the card student and then understanding the material deposited in the card via the pinched smart card, then the sanctuary catastrophe is inescapable. In authenticity, preceding assembly key(s) may be missing for a variability of explanations, counting equitation, corruption of material and the prearranged issue of that assembly key when the conference is torn depressed. Totaling this capability to A permits our prototypical imprisonment the hazard of the recognized key occurrence. To appraise the impairment of escape of attendant's long-term secluded important, the competence of knowledge waitperson's long-time isolated crucial is fortified with our challenger, counting it documents us to transaction with progressing discretion and key collaboration impress occurrence. Additionally, it is value observing that, in inaccessible user confirmation systems, for the sake of manageability, an operative is normally acceptable to optimal her own independence ID at will (at most tapering to a predefined prearrangement) through the registration period; the manipulator frequently inclines to indicate a uniqueness which is effortlessly recollected for her suitability. Therefore, these easy-to-remember independences are of squat entropy and thus can also be disengaged totaled by a contestant A inside polynomial period in the undistinguishable system with the watchwords. Henceforth, in recurrence, it is balanced and correct to accept that A can disconnected totaled all the (ID, PW) couples in the Cartesian Product Did*Dpw inside polynomial period. In dissimilarity, maximum of the planned dynamic-ID arrangements (i.e. manipulator's individuality is covered in meeting different would-be characteristics to deliver the stuff of operator secrecy),obviously undertake A cannot conjecture both ID and PW appropriately at the identical while. In other arguments, such dynamic-ID arrangements may be susceptible to disconnected watchword predicting occurrence

Sources	Similarity

SmallSEOTools

PLAGIARISM SCAN REPORT

Words	972	Date	August 15,2020
Characters	6857	Exclude Url	

0%	100%	0	43
Plagiarism	Unique	Plagiarized Sentences	Unique Sentences

Content Checked For Plagiarism

2.7.1.1 Evaluation Criteria As piercing out the building and refuge examination of watchword based verification arrangements with smart cards have an extensive antiquity, there is no common set of desirable sanctuary possessions that has been lengthily acknowledged for the construction of this type of preparations. Liao et al. made an effort to combine a huge set of ten necessary belongings, counting six sanctuary necessities, for appraising the blimey of a watchword based verification arrangement using smart card. Advanced on, Yang et al. contended that Liao et al.'s standards as some severances and planned a new-fangled set of only five principles for assessment the arrangements. Yang et al.'s standard customary is too theoretical (and thus unclear, not precise) to be accepted in physical claims. Virtually at the identical time, also obtainable additional slant of nine refuge necessities and ten wanted landscapes that an ideal watchword confirmation arrangement should accomplish. A shared article of together Liao et al.'s and Tsai et al.'s principles is that, the refuge provisions are originated on the displeasure confrontation theory of the smart cards, which may be unpredictable with the authenticity when captivating into explanation the state-of-the-art methods of side frequency cryptanalysis. More newly, Madhusudhan and Mittal piercing out that previous standards groups have dismissals and uncertainties and also planned a new principles set of nine sanctuary necessities and ten needed landscapes to appraise this type of arrangements. Since the refuge necessities of their standards are founded the non-temper confrontation supposition of the smart cards, their standards set is greater to other planned groups. Though, it nosedives to comprise some significant sanctuary necessities for a confirmation procedure with key arrangement, i.e., confrontation to recognized key occurrence, key collaboration impress occurrence and unidentified important portion occurrence. By succinct these previous educations, we put advancing a complete slant of twelve autonomous principles in rapports of user sociability and refuge that a watchword based distant user confirmation arrangement with smart card would content: C1. The waitron requirements not to preserve a folder for stowage the watchwords or some resultant standards of the watchwords of its patrons; C2. The watchword is unforgettable, and can be selected spontaneously and transformed nearby by the operator; C3. The watchword cannot be resulting by the advantaged superintendent of the waitron; C4. the arrangement is permitted from smart card damage occurrence, i.e., unlawful employers would not be brainy to naturally modification the keyword of the smart card, deduction the keyword of the operator by using keyword fathoming sessions, or reproduce the employer to login to the arrangement, even if the smart card is Got and/or clandestine information in the smart card is unprotected; C5. The arrangement can struggle numerous classes of cultured occurrences, such as disconnected watchword predicting occurrence, repetition occurrence, equivalent assembly occurrence, renunciation of provision occurrence, pinched verifier occurrence, impression occurrence, important cooperation impression occurrence, recognized crucial occurrence. C6. The arrangement delivers smart card cancellation with respectable repair ability, i.e., the customer can withdraw the smart card without altering her individuality; C7. The customer and the waitperson can launch a mutual meeting key throughout the confirmation procedure; C8. The arrangement is not disposed to the difficulties of clock harmonization and period postponement; C9. The arrangement delivers the stuff of appropriate incorrect watchword uncovering, i.e. the employer will be appropriate informed if he contributions mistaken watchword by fault in login chapter; C10. The arrangement can accomplish shared confirmation; C11. The arrangement conserves user obscurity to circumvent incomplete materials cape. C12. The arrangement delivers the stuff of advancing confidentiality. Principles usual is a modification and postponement of some beforehand planned obligation groups, it not only eliminates the discharges and reservations of the old responsibility groups, but also shortens cryptanalysis due to its compactness. It is not problematic to checkered that Madhusudhan and Mittal's standards set is completely encompassed into our customary. And it is also value noting that, dissimilar the principle assets planned by Tsai et al. and Liao et al, the principle regarding with presentation, which says "The arrangement must be well-organized and real-world", is not combined

principle regarding with presentation, which says "The arrangement must be well-organized and real-world", is not combined into our customary. The main motive is that, it does not appear to be quantifiable without mentioning to other connected arrangements, in other disagreements, separating it from the standards customary can make our set more tangible and decidable. Besides, the competence of an arrangement may be contingent on the application situation, while level headedness is mostly connected to the board submissions. Excluding this principle, all the other standards are encompassed into our customary. In assumption, our standards set are additional complete and tangible. 2.8 SECURITY ANALYSES In the following, we first describe an official safety classical for smart card grounded keyword confirmation arrangements, and then demonstration that our arrangement is safe in this classical underneath the prospects that the confusion determination prudently achieves like an accidental oracle and that the computational Diffie-Hellman problematic is challenging. In precise, our etiquette accomplishes advancing clandestineness stuff and refuge in contradiction of recognized key occurrence, key compromise impress occurrence. 2.8.1 Formal Security Model They describe some philosophies and recollection the BPR refuge classical where the opponent's capabilities are confirmed finished questions. Though, we do not use the innovative prototypical straight, but assume the reified variety planned by Bresson et al. with a few vicissitudes so that we can describe the singular protection provisions for watchword confirmation provisions using smart cards. We indicate the student to the ground-breaking identifications for more particulars. 2.9 INTRODUCTION TO GROUP KEY ESTABLISHMENT In command to advantage of protected collection leaning claims, numerous operators need to portion a secluded important, which is attained as the production of a Collection Key Formation procedure. The foremost objective of GKE is to launch a mutual significant amongst the sanctioned memberships of a collection, without revealing it to other gatherings. The sanctioned contributors to the procedure are also spoken as capable, genuine or advantaged

Sources	Similarity

SmallSEOTools

PLAGIARISM SCAN REPORT

Words	1000	Date	August 15,2020
Characters	6864	Exclude Url	

4%	96%	2	45
Plagiarism	Unique	Plagiarized Sentences	Unique Sentences

Content Checked For Plagiarism

2.10 CLASSIFICATION GKE procedures division into two courses: Collection Key Assignment and Collection Key Prearrangement. The foremost alteration amongst the two courses originates unswervingly from their meanings: GKT necessitates the reality of an advantaged get-together to choice and allocate the key, while GKA prepares not, the important being calculated as the consequence of the teamwork of sincere contributors via switched communications. Dissimilar GKA, in which the key is resultant only by the collaboration of interior assembly memberships, GKT documents the object that produces the important to be a foreigner as healthy (i.e. not a collection associate). This individual has numerous designations in the fiction, such as: Important Third Gathering, Significant Cohort Midpoint, Significant Delivery Epicenter or Cluster Supervisor [31]. The identification fluctuates rendering to the detailed meaning it accomplishes. For sample, it may happen an object that produces the important and an individual (separate or not) that allocates it to the sanctioned memberships. For the respite of this exertion we will principally mention to the KGC as a solitary party that achieves both key cohort and circulation. The KGC must be principal by all contributors as authentic in the intelligence that it chooses an additional key (a consistently accidental assessment that has certainly not been used beforehand) and does not disclose it to unreserved get-togethers. This conviction supposition is not compulsory for GKA procedures, which do not request the presence of an advantaged get-together to first-rate the important, but calculate it by equivalent involvement of the doyennes. However, notwithstanding of the GKE type, a conviction relative is compulsory: the competent contributors to an assembly conviction each supplementary that none of them divulges the collective significant. Then, the discretion of the etiquette is despoiled by nonattendance. We comment that throughout the implementation of a GKA etiquette, contributors do not conviction each additional and suspicious their associates may propose to get switch over the collection key charge. Owing to less conviction expectations, GKA frequently contents sturdier sanctuary. GKT undertakes (in universal) the being of protected communiqué networks among the KGC and each operator in the Users Recording Chapter: the long-lived important of a contributor frequently contains in a pre-shared clandestine (symmetric important or watchword) with the KGC. By dissimilarity, GKA do not execute such a statement: the long-lived answers of collection memberships are frequently community secluded couples' usages for validation (or occasionally, for unequal encryption).Concerning the influence type of the contributors to the GKA (a nonce or the long-lived important), GKA divided into [31]: Communicating GKA: Collection memberships underwrite to the important cohort with renewed standards for each conference (nonce). They necessitate switched communications amongst the contributors and consequently execute that all get-togethers are connected for the performance of the procedure. Non Communicating GKA: Collection memberships donate to the important cohort with their individual community long-live solutions. Instances comprise the innovative Diffe-Hellman procedure [32] and Joux tripartite procedure [30]. Unlike the Communicating GKA, their chief improvement is that an employer can regulate the mutual important even if the others are disconnected. GKT conventions are prime used in submission with national regulator. Grounded on the carefulness of the object that produces and allocates the key, GKT can additional division into [34]. 2.11 CENTRALIZED GKT It comprises a solitary individual that produces and allocates the important. Approximately of the disadvantages of this grouping comprise [35] (1) The KGC necessity be always connected (2) The KGC obligation preserve a protected communiqué network with each cluster associate; (3) The KGC could easily be the board of a DoS attack; (4) the computational authority of the KGC parameters the amount of manipulators he can handle. 2.11.1 Distributed GKT Despite all the mentioned advantages of GKA over GKT, one class or the other may suit best depending on the application needs or constraints (security requirements, computational resources and transmission costs). Due to the fact that parties do not necessary have to communicate between them (but only with the KGC, who performs most of the computation), the computational and transmission costs of GKT protocols are usually lower than those of GKA protocols. In addition, the design

computational and transmission costs of GKT protocols are usually lower than those of GKA protocols. In addition, the design of GKT is in general less challenging. Independent of the given classification, GKE may be considered in the context of static or dynamic groups: a static GKE does not provide special mechanisms for membership changes, while a dynamic GKE includes particular operations such as joining or leaving the group. In case that the authorized group of participants modifies, a static GKE must restart the process all over, while a dynamic GKE performs additional, but more efficient operations to update the group key and make it available and secure in the new settings. For the rest of our work we restrict to static GKE. 2.12 GKE BASED ON SECRET SHARING A general mechanism for defining GKE protocols is immediate KGC generates a fresh group key and sends its encrypted value under the appropriate key to each legitimate participant. Hence, any authorized user decrypts and finds the key, while it remains secure against unauthorized parties. We have assumed that an authentication mechanism exists, such that the KGC or the users cannot be impersonated and the message cannot be modified during transmission. This trivial solution becomes inefficient for large groups: KGC must perform m encryptions and send m messages, where m is the number of qualified participants. In case a symmetric encryption scheme is used to decrease the computational costs (rather than an asymmetric encryption scheme), a supplementary assumption appears: each registered group member must previously share a secret with the KGC. Underground distribution is used in GKE etiquettes to circumvent such drawbacks, permitting well-organized buildings: users may interconnect finished transmission frequencies only, the calculation of the important may entail in modest linear reckonings, the quantity of circles remnants continuous ever the less the collection scope. In addition, they present numerous welfares: an expedient method to discriminate amongst doyenne's influence within the collection, assignment of responsibilities by transient dividends to other contributors, collection verification instead of individual verification, dishonest uncovering and unassuming organization of collection sizing.

Sources	Similarity
Microsoft Word - art11OLIMID.doc A general mechanism for defining GKT protocols is immediate [7]: KGC generates a fresh group key and sends its encrypted value under the appropriate key to each legitimate participant. Hence, any authorized user decrypts and finds the key, while it remains secure against unauthorized... https://acad.ro/sectii2002/proceedings/doc2013-3s/11-OLIMID.pdf	5%

SmallSEOTools

PLAGIARISM SCAN REPORT

Words	974	Date	August 15,2020
Characters	7296	Exclude Url	

0%	100%	0	46
Plagiarism	Unique	Plagiarized Sentences	Unique Sentences

Content Checked For Plagiarism

2.13 SECURE KEY ESTABLISHMENT Protected communiqué over processor systems is frequently accomplished by incomes of encoding the replaced communications. The communications might be encoded by incomes of long-term community solutions (or long-term communal solutions). Though, the previous circumstance would necessitate that they portion the identical underground key which can be attained by income of some protected key formation procedure. By resources of such etiquettes, two or more persons can create communal underground cryptographic answers over unconfident systems. The procedures can be grounded on clandestine important cryptography or communal important cryptography. Due to distribution of long period underground solutions amongst a quantity of operators is an unreasonable supposition, most important founding procedures that is based on communal key (a.k.a. symmetric key) cryptography necessitate connected TTP. Henceforth, each employer would portion an underground important with the TTP, and all key formation communications would go complete the TTP. Kerberos [34] and the symmetric significant decorum of Needham-Schroeder [35] are two well-known specimens of significant launch conventions created on collective underground solutions. As it would be a problematic to allocate and launch new communal explanations to new operators over an unconfident system if a key is not previously communal amongst the new operator and the TTP. The benefit of community key symbols is popularization of key organization and eradicating the essential for a connected TTP. This upsurges significantly the usability for procedures grounded on community key symbols, which have consequently developed for additional significant than symmetric important procedures. Most community important etiquettes are grounded on a few well-known difficulties in quantity philosophy like the Separate Logarithm Problematic, the thoroughly associated Diffie-Hellman Badly-behaved, and the Factorization Unruly (i.e., the struggle of factorizing numbers self-possessed of two very great hey days). For specimen, the RSA communal crucial cryptosystem is founded on the Factorization Problematic, and the ELGamal communal important cryptosystem [36] is grounded on the two thoroughly connected Diffie-Hellman Problematic and the Disconnected Logarithm Problematic. All refuge procedures in this proposition are community key-based. Key formation etiquettes can fundamentally be separated into key handover conventions and crucial arrangement conventions. Key assignment is anywhere one thing produces the underground crucial and dispenses it privately to one or more manipulators. Key contract is anywhere two or more contributors that "decide" on a clandestine key by correspondingly causative to the worth of the well-known important. Rendering to the quantity of contributors, such etiquettes are considered as two-party and multi-party conventions. 2.14 GROUP-ORIENTED CRYPTOGRAPHIC PROTOCOLS Protected collection communiqué mentions to the situation in which a collection of contributors can interconnect steadily over some processor system in such a technique that the switched communications would be incomprehensible for foreigners and non-pertaining operators. Meeting key founding procedures (also recognized as multi-party key founding procedures) permit a quantity of workers to found a communal meeting important where of protected communiqué over unconfident processor systems can be attained by encoding the switched communications. Collection concerned with key arrangement is a unusual circumstance of protected multi-party calculation, anywhere n contributors, U= {P1;.....Pn}, calculate the consequence of some meaning f(x1;:::;xn) and where each Pj €U grasps a underground input xj . The problematic is how to calculate f without figure-hugging their clandestine participations to any other get-together, counting the other contributors. The meaning might be any occupation attractive any contributions

where the additions are showed over a dispersed system. A comparatively great period of graded cryptographic systems is identified as Hierarchical Admission Regulator. The foremost drawback of Ranked Admittance Switch arrangements is that such arrangements fundamentally deliver calculation of long-term, predefined ranked keys. This income that the new answers have to be disseminated for every meeting from the important midpoint. In dissimilarity, protected graded collection communiqué could be attained by incomes of graded important formation etiquettes. Such procedures enable protected

communique could be attained by incomes of graded important formation etiquettes. Such procedures enable protected formation of an amount of sitting answers in arrangement with the assumed quantity of operator heights. An indispensable refuge stuff is that operators of a assumed equal can calculate the ranked meeting solutions affecting to their individual and fundamental refuge heights, while it is computationally infeasible to calculate graded meeting answers of super imposing refuge heights. 2.15 INFORMAL SECURITY REQUIREMENTS A GKE procedure ought to content a set of possessions, which we nonchalantly recollection next. Important discretion (also called important discretion, important confidentiality or non-disclosure) [37], [38]promises that it is (computationally) infeasible for a challenger to calculate the collection important. The stouter concept of identified important refuge guarantees that key discretion is preserved even if the aggressor someway accomplishes to acquire assembly answers of preceding assemblies. Retrograde confidentiality [39] marmalades the discretion of forthcoming answers notwithstanding the opponent's activities in the past assemblies. Consistently, advancing clandestineness [39]executes that the challenger movements in forthcoming battings of the procedure do not negotiation the confidentiality of preceding assembly explanations (i.e. a important leftover safe in the forthcoming).Important collection must please precise belongings. Key cleanliness necessitates that the collection important has certainly not been secondhand before. The connected notion of important individuality executes that no association happens among solutions from dissimilar assemblies; this income that (collaboration between) official contributors to different sittings of the etiquette cannot unveil meeting answers they are unlawful for. In totaling, key haphazardness licenses significant in-distinguish aptitude from an accidental quantity and hence important impulsiveness. Two additional significant refuge necessities concerning the key worth happen: key truthfulness which confirms that no opponent can adjust the collection important and crucial steadiness, which averts dissimilar companies to take dissimilar answers. Collection affiliate confirmation characterizes a compulsory illness for assembly cryptographic etiquettes. Object confirmation authorizes the uniqueness of a contributor to the procedure to the others. Correspondingly, unidentified key portion flexibility confines an operator to trust that the important is communal with one get-together when in fact it is communal with additional. Important negotiation parody flexibility [40]avoids an aggressor who possesses the long-lived key of a contributor to imitate other gatherings to him.

Sources	Similarity

SmallSEOTools

PLAGIARISM SCAN REPORT

Words	965	Date	August 15,2020
Characters	6946	Exclude Url	

2%	98%	1	40
Plagiarism	Unique	Plagiarized Sentences	Unique Sentences

Content Checked For Plagiarism

2.16 LITERATURE REVIEW Let's discuss works proposed by various researchers by S. Bellovin and M. Merritt gives the first fruitful password-authenticated key arrangement means were Encrypted Key Exchange means described. Although numerous of the first approaches were defective, the enduring and greater forms of EKE efficiently increase a shared keyword into a collective key, which can then be used for encryption and/or message verification. Procedures for genuine key exchange permit two gatherings to produce a communal, cryptographically sturdy key while collaborating over an uncertain network below the comprehensive Regulator of an opponent. Such procedures are amongst the most extensively used and important cryptographic primitives; indeed, arrangement on a common key is essential before higher-level errands such as encoding and memorandumcorroborationdevelopedimaginable.Watchwordgroundedauthenticimportantconversationmeasuresdocument two operators to harvest a mutual, cryptographically-strong key originated on an original, low-entropy, common underground (i.e., a watchword). Katz, Ostrovsky, and Yung (KOY) [42] established the chief well-organized PAKE procedure with a resistant of refuge in the normal perfect. The technique was unconventional anxious by Gennaro and Lindell (GL), who contributed an overall outline that incorporates the innovative KOY procedure as a singular circumstance. These procedures are protected smooth underneath harmonized presentations by the similar get-together, but necessitate a shared orientation thread. Though this might be fewer attractive than the unadorned classical, dependence on a CRS prepares not seem to be a thoughtful disadvantage in repetition for the disposition of PAKE, where mutual strictures can be hard oblique into an application of the etiquette. The KOY/GL outline necessitates a CCA protected encoding arrangement (such as Cramer-Shoup cryptosystem with a connected straight projective hash connotation and its postponements necessitate four rounds in command to achieve common confirmation. Virtually all succeeding effort on well-organized PAKE in the normal prototypical can be watched as spreading and construction on the KOY/GL outline. A different PAKE technique in the CRS faultless is assumed by Jiang and Gong, later preoccupied and widespread by Groce and Katz [43]. Associating to KOY/GL outline, the new JG/GK outline only necessitates a CCA protected encoding arrangement, and a CPA protected encryption preparation with a linked horizontal projective confusion connotation. It also achieves shared corroboration in three groups. In their exertion Groce and Katz quantified their summary will expressively spread ability once foundation the protocol on framework expectations. Katz and Vaikuntanathan first instantiated the KOY/GLPAKE process under framework outlooks. In teaching to chew into the JG/GK's summary, we use an projected framework grounded SPH and an blunder amending code (ECC) to do the occupation of an careful lattice-based SPH [44]. In 2009 byS. Wanga, Z. Cao, K.-K. Choo, and L. Wangthe first proper refuge classical for authentic key exchange conventions between two festivities. The latter has been extended to the password-based setting with security analyses of the above 2-party password-based key exchange, under idealized assumptions, such as the random oracle and the ideal cipher models. Password-based arrangements, provably protected in the normal classical, have been recently proposed but only for two parties. papers considered password-based protocols in the 3-party setting, but none of their schemes enjoys provable security. In fact, our general edifice appears to be the first provably-secure 3-party password-based authentic key exchange etiquette [45]. In 2009 by D. XiaoFei and M. Chuan Gui introduce additional connected line of investigation is authenticated key conversation in the 3-party location. The primary exertion in this extent is the etiquette of Needham and Schroeder which stimulated the Kerberos disseminated organization. Later, Bellare and Rog away familiarized a prescribed refuge classical in this situation length ways with an edifice of the primary provably protected symmetric crucial grounded key circulation arrangement. In this weekly, we reflect the unusual but vital case in which the underground explanations are pinched from a unimportant set of ethics [46]. In 2010 by Pinpointed out Yang et al.'s arrangement is susceptible to important cooperation occurrence. Astonishingly, we originate Yang et al.'s arrangement still

arrangement is susceptible to important cooperation occurrence. Astonishingly, we originate Yang et al.'s arrangement still cannot accomplish its demanded foremost refuge goalmouth by representative a disconnected watchword predicting occurrence in Supplement A, and finished the refuge examination of Yang et al.'s arrangement, some refinements and contests in conniving this type of arrangements, dissimilar from the outdated watchword grounded confirmation, are exposed. Notwithstanding of this, Yang et al.'s prescribed adversary traditional does incarceration the scrupulous two influence corroboration of shrewd card-based keyword authorization preparations: only with both the clever card and the accurate keyword can a user communicate out the smart-card-based keyword authorization procedure absolutely with the isolated corroboration waitron [47]. In 2012 by Wang, Y.G. pragmatic that the preceding identifications in this portion current occurrences on measures in previous identifications and recommend new measures deprived of accurate sanctuary clarification (or smooth a security conventional to completely identify the functional intimidations), which underwrites to the foremost source of the overhead disappointment. Therefore, Wang accessible three classes of protection models, precisely Type I, II and III, and additional forthcoming four touchable organizations, only two of which, i.e. PSCAb and PSCAV, are necessitated to be threatened underneath the severest classical, i.e. Type III refuge classical. The type III classical will be studied advanced in Segment 2. Though, PSCAb necessitates Weil or Tate combination processes to protect touching disconnected foreseeing occurrence and might not be suitable for administrations where combination procedures are painstaking to be too luxurious or infeasible to instrument. Furthermore, PSCAb agonizes from the well-known crucial escrow problematic and deficiencies some needed structures such as indigenous watchword apprises, reparability and user obscurity. As for PSCAV, in Appendix B, we will validate that it immobile cannot achieve the wanted sanctuary goalmouths and is feeble to a disconnected keyword foreseeing occurrence and extra sessions under the Type III refuge classical. The chief influence, a vigorous and well-organized procedure is available to handle with the acknowledged imperfections and it is legally demonstrated to be protected in the Type III sanctuary prototypical [48].

Sources	Similarity
An Efficient Trust Model for Online Application using 2-Factor... password-based schemes, provably secure in the standard model, have been recently proposed but only for two parties. papers considered password-based protocols in the 3-party setting, but none of their schemes enjoys provable security. in fact, our generic construction seems to be the first... https://www.ijsr.net/archive/v6i2/ART20171110.pdf	4%

SmallSEOTools

PLAGIARISM SCAN REPORT

Words	312	Date	August 15,2020
Characters	2069	Exclude Url	

0%	100%	0	16
Plagiarism	Unique	Plagiarized Sentences	Unique Sentences

Content Checked For Plagiarism

In 2009 by Xu, J., Zhu, W., Feng, D. planned a general edifice agenda to adapt the conservative provably protected PAKE procedures to shrewd card-based forms and additional intentional an innovative arrangement to validate its efficacy. The new structure is demanded to be locked and can gratify all their projected principles. In the subsequent, we will expression that their outline is essentially disposed to disconnected keyword foreseeing occurrence, thus retreating the power completed that the new structure is protected smooth if the secret statistics packed in smart card is exposed by the opponent[49]. Zubaile Abdullah, Madihah Mohd Saudi and Nor Badrul Anuar proposed a new and efficient technique for the Mobile Botnet Detection using Proof Concept [50]. This tabloid offering an impermeable of notion on how the bot systems and the continuing exploration to perceive and answer to the movable botnet competently. Discovery of botnet spiteful movement is completed complete an investigation of Cruse wind Botnet cipher using opposite manufacturing development and stationary investigation practice. K. Nirmal et. al's proposed a new system based on 3 Factor Authentication for Counter-attack Phishing [52]. Since Phishing is an Online Security attack, hence the chances of personal, financial or password data loss is maximum. Here in the paper an improved Anti Phishing framework is implemented known as Phish-Secure. It is based on the concept of Image Similarity Detection for the Identification of replica of the Site. In the algorithm 3 Factor Authentication techniques is proposed which detects and prevents all types of phishing attacks. R. Manjusha et. al's has given a new Security framework for E-commerce applications [53]. Here in this paper author has implemented combination of false hit database algorithm and nearest neighbor algorithm to provide security of E-commerce applications. A new framework has been implemented which is not only based on Web Mining Structural Analysis but it includes decision analysis and security analysis.

Sources	Similarity

SmallSEOTools

PLAGIARISM SCAN REPORT

Words	1000	Date	August 16,2020
Characters	6704	Exclude Url	

0%	100%	0	44
Plagiarism	Unique	Plagiarized Sentences	Unique Sentences

Content Checked For Plagiarism

3.1 PROBLEM STATEMENT Security in various E-commerce Applications includes an efficient framework in Information Security especially in Computer security and Data Security and other online transactions in E-commerce applications. Security in E-Commerce application plays an important role for the secure and scalable transaction which includes various dimensions such as security-integrity, Confidentiality, Non-repudiation, Privacy etc. Hence for the Security of Online Transactions in E-Commerce based application various Security algorithms are implemented. Although these Security algorithms are efficient and provides Security from various attacks but Data Storage during the transactions and Computational time of the algorithms is also important. The Existing architecture proposed for the security of online e-transactions in web applications provides security from different attacks and is efficient in terms of computational parameters, but there are certain issues which need to be overcome such as: 1) Security Prevention from different attacks during Online Transactions in Web Mining especially in E-commerce Applications: Security is an important concern in online transactions in E-commerce based web applications. Although different types of authentication algorithms are implemented for the prevention of different types of attacks possible, but some algorithms fails to prevent from such attacks. 2) Increase use of Computational Cost at the Client and Server Side: During implementation of various authentication algorithms for online transactions security is not the only concern but other factors such as Computational cost is also important which decides the cost of the infrastructure; since more is the Computational Cost complexity of the system also increases. 3) Increased Communication Cost and Time: Communication time is also another important factor during online transactions, whenever any online transaction takes in E-commerce application the communication time can be reduced so that the chances of attacks also reduces. 4) Reduce Storage Cost used during use of Smart Cards: The Existing methodology implemented for the Security of Online Transactions using Smart Cards based Authentication is efficient but the concept takes more Storage which increases the Cost of the System, hence an efficient Smart Card based Authentication needs to be implemented which not only provides efficient prevention from attacks but also provides reduced Storage Cost. 3.2 OBJECTIVES With the advent of Web mining and their various application areas such as in E-commerce the data sensitivity also increase and hence is the privacy of data. However various security algorithms are implemented to enforce security and privacy in E-commerce application. The main purpose of this work is as follows: 1. To implement Secure & Efficient technique in various Applications. 2. To reduce time complexity and space complexity. 3. Implementation of efficient authentication to secure from various attacks. 4. To reduce Time Computation of the framework. 5. To reduce Communication Cost & Time. 3.3 PAKE Password Authentication based on Exchanging Key (PAKE) procedures permit two objects to agree on a shared sitting key which is based on an unforgettable keyword. The foremost refuge objective of these etiquettes is providing protection against keyword predicting bouts. Two-party password-based authenticated key exchange (two-PAKE) process is rather useful for client-server buildings. Though, in large-scale client-client message settings where a user requirements to interconnect with many other workers, Two-PAKE procedure is very tiresome in key organization that the quantity of keywords that the user would need to recollect. 3.4 PROBLEM SCENARIO WITH EUROGRABBER ATTACK The Eurograbber attack starts when Trojan's infect the User's computer and the attack starts communication with the bank. In the Second phase attacker can try to steal the mobile number of Customer and hence attack the devices. During the Second Phase when Customer logging into his bank account, the attacker initiates a funds transfer from the user's account to attacker's account. In the last phase Bank communicate a Transaction Authorization Number (TAN) via SMS. The attacked source on the Customer's phone captures the SMS and reflect back to the attackers to inclusive an illicit operation. When User tries to reply back to the Phishing email, DDoS or click fraud tempts the user to click on the spurious url. The Trojan is then downloaded on the restricted system and Trojan waits for the User to login into account. As soon as the Customer Logins into his bank account Trojan Virus obstruct the session and insert a script

login into account. As soon as the Customer Logins into his bank account Trojan virus obstruct the session and insert a script into the customer banking page this script notify the customer regarding "security update" and provide instruction to proceed further. 3.5 OVERVIEW OF PHISHING ATTACK The evolution of 'Phishing' introduced with the advent in 1990s. The Stealer used to use the word 'pha' to reinstate the word 'fa' so as to generate new terminology in the hacker's society, since they commonly bait by phones. It is a latest word emerged from 'fishing', the attackers lures the customer to visit a forged location by distribution them forged e-mails (or instantaneous posts), and silently get fatalities private data for example user name, password, national security ID, etc. This mainstream of the data afterward might be utilized for possibility focus promotions alternately much personality confirmation strike (e.g., transfer cash from victimized people's bank account). Phishing may be a manifestation from claiming web cheating whereby phisher embrace social building schemes Toward sending instant messages-mails alternately internet promoting will charm clients will phishing sites that pretend as truthful sites so as on trap people under uncovering their insightful information [1]. Phishing e-mail may be a unique kind about spam message. Such e-mail starting with a legitimate organisation or bank. Consequently, through an immerse link inside the email, those phisher endeavours to redirect clients on forged sites that need aid outlined on dishonestly get money related information for example, such that usernames, passwords, Also number of credit card. One of the key objectives of phishing is to dishonestly carry out deceitful financial transactions at the behest of users by using a counterfeit email that consisting a URL indicating to a forged site impersonate as a government unit or an online bank. A phisher trick victim to give his full name, Number of social security & address, which may be useful for applying to produce credit card on behalf of the victim.

Sources	Similarity

SmallSEOTools

PLAGIARISM SCAN REPORT

Words	868	Date	August 16,2020
Characters	5627	Exclude Url	

0%	100%	0	40
Plagiarism	Unique	Plagiarized Sentences	Unique Sentences

Content Checked For Plagiarism

3.5.1 Types of Phishing Attack These attacks can be categorized into different types as per the way assault is done. Various types of attacks define by researcher has been described below. Deceptive Phishing- phisher sends ample email along with a message. Users are affected by phisher to visit the link. For example phishing email says that some updating is needed with recipient's account at financial company and requests the recipient to visit the website link to update his details. After that a statement may receive by the recipient which state that his account is at risk and offering to register him to defraud program Malware-Based Phishing- In Malware-based phishing, user's machine which run the malicious software. An email attachment form or a downloadable file can be a malware containing protection vulnerabilities. Web Trojans - They pop-up imperceptibly when other users are simultaneously trying to login. They group together the user's secret data locally and then send it to the phisher. Hosts File Poisoning-- As soon as a user enter a URL should visit a webpage it must primarily a chance to be translated under a IP address preceding it is transmitted in the web. The foremost part of SMB users' PCs running an operating system becoming better these "host names" in their "hosts" file prior to undertaking a DNS lookup. By "poisonous" the hosts file, phisher have a counterfeit address transmitted; unenthusiastically user takes this address which is a counterfeit site where their data can be sniffed. System Reconfiguration Attacks-This type of attacks occurs due to wrong compilation of security configurations. The attacker tries to breach and hence capture the sensitive data over applications. In Today's Web based application it is not only the responsibility of developers to implement correct security configuration but also Admin and Network Administrators. DNS-Based Phishing –DNS based phishing is known as pharming, in this type of phishing phisher alter the company's host file or DNS so that requirements for URLs or service name revisit a counterfeited lecture to and sequential transportation are aimed at to a phishing site. Content-Injection Phishing-It explain those circumstance the place attacker trade and only the data of a real site for false substance outlined to misdirect or mislead those client under surrendering their secret data to the attacker. For instance, phisher willtries to inject pernicious regulations to project user's secrets or cover which can clandestinely assemble in sequence and distribute that information to phisher. Man-in-the-Middle Phishing-In this category of attack source positions themselves in between real website and user. They verify the prevalence of in sequence creature entered by user but prolong to bypass so that client's dealings are unaffected. After they utilize the major data or gathered when those users will be not dynamic on the framework. Search Engine Phishing- Happens when phishers makes sites for alluring (often a really attractive) sounder give and bring them numbered authentically with explore mechanism. Client find the sites in standard itinerary of penetrating for invention or services Furthermore are stealth under surrendering their data. To example, defrauder plan counterfeit banking sites advertising bring down credit expenses or preferred enthusiasm rates over different banks. Victim who use these sites or make additional from investment charges are encouraged with exchange obtainable financial records What's more undertaking with surrendering their details. 3.5.2 Procedure Commonly, this attack are performed with the subsequent four steps in which phisher try to fraud the user by counterfeited website embedded in the email. 1. Phishers establish a counterfeit position which is precisely like real Website, plus put up the app server, generating those DNS server name, and constructing the analogous pages of web to the purpose site etc. 2. Propel immense measure of stealth e-mails to destination clients in the name of those justifiable organizations and enterprise, wearisome to entice the budding wounded to stopover their Websites. 3. The e-mail is received by receiver and opens it then clicks the spoofed link in e-mail, and enters required information. 4. Phishers filch the personal data and performing their scam like transferring money from the victims account. 3.5.3 Life Sequence of Phishing Email The latest explore result convergence on evaluating phishing attacks only depend on electronic mail. Life sequence of phishing generates with a large bulks that try to entice the bearer to click an incorporated email linkage. This segment of phishing is approximating to fishing. As an alternative of with fishing persuade and stroke to hold a fish, a phisher sends out enormous

approximating to fishing. As an alternative of with fishing persuade and stroke to hold a fish, a phisher sends out enormous emails with anticipation that any of the Users will rejoinder the email by clicking the email link. Normally the email seems true and will comprise a corporation logo of an accepted monetary establishment and a revisit lecture of the genuine corporation. Desire of the phisher is to lure to appear more authentic so that the victims will response it without thinking. The responsibly of Message Transfer Agent is to sending and receiving mail between systems using SMTP. For receiving a message from an MTA are conscientious by Message Delivery Agent and assembling can be acknowledged by the confined classification (e.g. forwarded to a mailbox). MUA: Mail User Agent is such a agenda in which conclusion Client read mail and progression mail. Characteristic examples comprise MS-Outlook etc.

Sources	Similarity

SmallSEOTools

PLAGIARISM SCAN REPORT

Words	950	Date	August 16,2020
Characters	6315	Exclude Url	

0%	100%	0	44
Plagiarism	Unique	Plagiarized Sentences	Unique Sentences

Content Checked For Plagiarism

CHAPTER 4 PROPOSED METHODOLOY 4.1 PROPOSED METHODOLOGY The Proposed methodology implemented here is based on the concept of Two Factor Authentication which provides Security prevention from various attacks especially in Online Web Transactions. The Methodology implemented here works in two phases 1) Authenticating the validity of the User by allocating a challenge value 2) Improved Smart Card based Authentication using Elliptic Curve based Encryption and Data Validation. The Proposed methodology implemented works on the basis of the following - Whenever any new Customer performs any online Transaction on Web, he needs to do handshaking with the Server using shared Challenge value over secure channel. Handshaking between customer and server is done based on challenge value and secrete Shared Password. The Challenge value is limited for a particular Session only. After First Factor Authentication, the Customer needs to Register on Server and authenticate using Second Factor Authentication. This phase contains various Steps such as Login / Register / Verification / Password Change. 4.1.1 First Factor Authentication using Challenge Handshaking If in Online Transaction Client want to communicate with Server, then first client sends a request to the server, the server responds. The server asks for the client to enter a challenge value. The server in respond to challenge value generates a master key using MD-5 hashing technique and responds client to enter his unique password. Since every client has its own password, so client enters his password and with the challenge value and password client calculates a master solution and respond back to the server. The server verifies both keys and authenticate client. First of all Customer will Sends request to the Server for the computed Challenge Value. The Web Transaction Server will take the Challenge Value. Server Computes Time Stamp T1. Server will now take the Password value. Server Sends Challenge Value with Time Stamp T1 to the Customer. Customer then receivers the Challenge Value with Time Stamp T1 from the Server. Customer then Computes Current Time Stamp T2. On the basis of these Time Stamps T1 & T2, Customer calculates total transmission time. Total_(transmission time)=2*(T2-T1)+processing time Customer now takes password and determine MD5 hashing function on challenge value + password +total transmission time. Customer computes MD5 hashing on this data. Customer will sends this data to Server. Server received the data D1 from Customer and computes timestamp T3. Server determines (challenge value + password + T3). Server also determines MD5 hashing on (challenge value + password + T3). If it matches then session is valid. Cheek whether the password valid or not If valid send allowed else send not allowed else session expires. Customer will show whether session expires or not. If not expired then whether password valid or not. 4.1.2 Second Factor Authentication using Improved Smart Cards The Second factor authentication involves use of Smart Cards for only one time Registration on the Server and Sending and receiving Transaction with high level Security with Asymmetric based Encryption. 4.2 ELLIPTIC CURVE CRYPTOGRAPHY Elliptic Curve Cryptography is a technique which is based on the notion of Elliptical curve assumption which is based on Hard Logarithmic Problem used to generate easier and faster with effective Cryptographic Keys. Elliptical Curve based Cryptography is used for the cohort of Keys by using the Elliptic Curve Equations. Elliptic Curve Cryptography yields a level of Security from 164-bits keys to 1024 bits depends on the System Requirements. The General Equation of the Elliptic Curves is given as: 4.2.1 Key Generation using Elliptic Curve Cryptography Since ECC is based on Asymmetric Key Cryptography hence is used to generate both pairs of Public and Private Keys for Online Transaction. The Information Possessor of the Web uses the Server's communal key for the encryption of the Message and Server uses its private key for decryption. Let 'n' is the maximum limit and must be a prime number, select a number

'S'(private key) within the range of 'n' which is the private key for the Data Owner, hence using this secluded key and the Improper Opinion 'B' (which is any point on Curve) public key 'P' is generated. P=B*S 4.2.2 Encryption using Elliptic Curve Cryptography For the Encoding process to be performed using ECC, community, and isolated key pairs are used. Suppose a Message 'M' needs to be encrypted using ECC, take any point 'm' on the point 'M' on the Curve of Elliptical equation 'E'. Choose any arbitrary position on the Elliptical Curve 'r' within the range from [1 (n-1)] cr=Sk 1 (M) 4.2.3 Decryption using Elliptic Curve

any arbitrary position on the Elliptical Curve 'P' within the range from [1-(n-1)]. c=3k_1 (M) 4.2.3 Decryption using Elliptic Curve Cryptography For the Decryption of the Cipher Text 'C' the following operations needs to be performed at the Server side of the Online Transaction. M=□PK□_2 (c) 4.3 WORKING OF PROPOSED METHODOLOGY New Client Registration Segment-In the registering segment, client Ui requirements to record in inaccessible server S. Primarily client indicates his/her IDi and PWi. Previously catalogue on Server, recording consultant calculates hash (IDi) and hash (IDi||PWi) and guides to inaccessible server S over a secure frequency. The computed values are encrypted using characteristic based Encoding with Elliptical Curve based solution production and send to Server. Upon reception the registering claims from User Ui. Server Decrypts the Data using his Public Key and verifies the message. Server S analyzes same criticisms associated to the User Ui. S calculates □PA□_i=Hash(□ID□_i).xor.hash(X_s ||hash(□ID□_i)) □PB□_i=□PA□_i.xor.hash(□ID□_i ||□PW□_i) □PC□_i=hash(□PA□_i) □PD□_i=hash(□ID□_i ||□PW□_i).xor.hash(X_s) And stowed a quantity in the elegant tag recollection and subjects this elegant certificate to Client Ui. This smart certificate is transported to Client Ui during a protected network. Authentic Client Login Segment-This segment generates the capability of a protected entering to the client .client requirements to admission same services on distant server S. first it improvement the admittance correct on the isolated server S.

Sources	Similarity

SmallSEOTools

PLAGIARISM SCAN REPORT

Words	457	Date	August 16,2020
Characters	3407	Exclude Url	

0%	100%	0	22
Plagiarism	Unique	Plagiarized Sentences	Unique Sentences

Content Checked For Plagiarism

Confirmation/substantiation segment - Upon receiving the login application announcement {PFi, PEi, PCid, Tu, hash (IDi)}. Server authenticates the authority of time impediment between current (Tu') and previous time. Where Tu' is the journey period of the message/data. Current time (Tu')-previous time (Tu) ≤ difference time (ΔT)where ΔT notates expect convincing time distance for communication impediment. Then server takes the entered appeal and go to subsequently progression, or else the server discard entered appeal. Server calculates – □PA□_i^*=hash(□ID□_i).xor.hash(X_s ||hash(□ID□_i)) □PR□_i^*=□PA□_i^*.xor.□PC□_i G=hash□(□ID□_i ||□PW□_i)□^*=□PC□_id.xor.□PR□_i □PD□_i^*=hash□(□ID□_i || □PW□_i)□^*.xor.hash(X_s) And computes □PF□^*=hash(□PA□_i^* ||□PD□_i^* ||□PR□_i^* ||T_u) And verifies to check PF and PF* are comparable. If not comparable then decline the entered appeal. If identical, then server S calculates– PFs = hash (hash (IDi) || PDi || PRi || Ts) somewhere, current (Ts time) is isolated server in progress instance and throw recognize message {PFs, G, Ts} to user Ui. Upon receiving concede message smart card calculates G^*=hash(□ID□_i ||□PW□_i) □PF□_s^*=hash(hash(□ID□_i)||□PD□_i ||□PR□_i ||T_s) Verifies that parameter (G) =G*and PFs = PFs* are identical or not with reciprocated substantiation progression. Here both Server and Client authenticate to each further. If they are identical then tag makes conference solution (Sk) and both Server and Client contribute to it. S_k=hash(hash(□ID□_i)||T_s ||T_u ||□PA□_i Otherwise dismiss to over entering progression. Secret code modifies Phase-This stage is concerned every time Client U needs to modify the password (PW) with some more sophisticated Password (PWnew). Client U then enters his generated smart card and enters new (ID*) and new (PW*) and appeal to modify secret word. The tag then verifies parameter(C) = C* are comparable. If it is correct then Client U is a genuine owner of the tag. On the other hand tag asks the Client Ui to participate new code word PWnew. After inward bound the new secret word the tag calculate- B_new=□PA□_i.xor.hash(□ID□_i || □PW□_new)and D_new=hash(□ID□_i ||□PW□_new).xor.hash(□ID□_i ||□PW□_i).xor.□PD□_i modify parameter (B) with Bnew and D with Dnew in smart tag memory. 4.4 FLOW CHART OF PROPOSED METHODOLOGY The figure 4.4 is the proposed structure of the methodology implemented for the security of Web Mining based Application especially in E-commerce. The planned procedure implemented here works on the framework of Authentication on Two Factor which provides Security from attacks especially in Online Web Transactions. The Methodology implemented works on two phases 1) Assigning the validity of the User by allocating a challenge value 2) Improved Smart Card based Authentication using Elliptic Curve based Encryption and Data Validation. The proposed technique implemented here prevents from numerous types of security attacks such as replay attack and identity disclosure attack or outsider attack and provides security from various dimensions such as security-integrity, Confidentiality, Non-repudiation, Privacy etc. The two factor verification that we proposed here takes low Computational Cost and Computational Time.

Sources	Similarity

SmallSEOTools

PLAGIARISM SCAN REPORT

Words	978	Date	August 16,2020
Characters	5825	Exclude Url	

0%	100%	0	47
Plagiarism	Unique	Plagiarized Sentences	Unique Sentences

Content Checked For Plagiarism

CHAPTER 5 IMPLEMENTATION & RESULT ANALYSIS The Minimum software and hardware requirements for implementing the problem statement is given below:- 5.1 HARDWARE REQUIREMENTS 1. RAM 512 MB 2. Processor Dual core or above 3. Hard Disk 5GB 4. Smart Cards 5. Mouse 6. Keyboard 5.2 SOFTWARE REQUIREMENTS 1. JDK 1.6 or above 2. NetBeans 6.9 IDE 5.3 EXPERIMENT DESIGN The Figure 5.1 is the output screen of the First Factor Authentication, where Client wants to interrelate with the Server. Server Sends message to Client asking for whether to Send message or not. If Client says 'y' yes to send message to Server. The Figure 5.2 is the output screen when Client requests to Send message to the Server. Server generates Unique Token for the Client using MD-5 hashing and asks for the client to send his master token key. The Figure 5.3 is the output screen where Server asks Client to send his master Token for the Verification of the client. The Client in response enter his secrete Unique password and Generates Master Secrete Key and Send to Server for Verification The Figure 5.4 is the output Screen of the Authentication using Second Factor using Smart Cards. Here in the Authentication using Second Factor consist of two phases, if User is already registered or he is new Users and wants to interrelate with Server. The Figure 5.5 is the Registration phase if any new user requests to Send Message to Server. User enters his ID and Secrete Password and in response to ID and Password two parameters are generated as shown below. The First Parameter is computed by applying Hash Function on ID and Second parameters is generated by applying Hash Function on the Concatenation of (ID || Password). The respective generated parameters are then Send to Server. Here Hash Functions such as MD-5, SHA-1, SHA-256 can be used. The Figure 5.6 is the Registration phase if any new user requests to Send Message to Server. User enters his ID and Secrete Password and in response to ID and Password two parameters are generated as shown below. The First Parameter is computed by applying Hash Function on ID and Second parameters is generated by applying Hash Function on the Concatenation of (ID || Password). The respective generated parameters are then Send to Server. Here Hash Functions such as MD-5, SHA-1, SHA-256 can be used. The Figure 5.7 is the Output of the Smart card Storage which consists of id and Password and Four Parameters A, B, C, and D. These Parameters are computed by the Computation from Server. The Figure 5.8 is the output Screen of the Server where the Computation of different parameters takes place. Here Computation of Four Parameters A, B, C and D takes place and some other parameters also. The Figure 5.9 is the Output of the Smart card Storage which consists of id and Password and Four Parameters A, B, C, and D. These Parameters are generated by the Computation from Server. The Figure 5.10 is the output screen of the Client Login Phase, when Smart Card is generated by the Server for Client. When Client wants to Login he needs to enter his ID and password and on the basis of his ID and Password certain Computation is done and verifies that the Smart Card belongs to Users or not. The Figure 5.11 is the output Screen of the Server where the Computation of different parameters takes place. Here Computation of Four Parameters A, B, C and D takes place and some other parameters also. The Figure 5.12 is the output screen of the Client Login Phase, when Smart Card is Generated by the Server for Client. When Client wants to Login he needs to enter his ID and password and on the basis of his ID and Password certain Computation is done and verifies that the Smart Card belongs to Users or not. 5.4 EXPERIMENTAL RESULT ANALYSIS The analysis of various types of attack prevented by the proposed scheme is implemented in this section and represented with various tables. The Planned procedure implemented here as 2 Factor Authentication prevents from various types of attacks. 5.4.1 Replay Attacks A replay attack (also known as playback attack) is a type of network attack where transmission of valid data can be access in an unauthorized or can be delayed. The primary way of carried out is using originator or an adversary who analyzes the data and send it again, probably as part of a masquerade attack by IP packet substitution. The scheme implemented here securely prevents any type of replay attack in E-Commerce applications. Since the concept is based on Two factor Authentication and lard logarithmic, hence if an attacker tries to attack any online transaction it can attack using some unwanted regular applied keys. Mathematically replay attack is, U_A : hash(□PW□ ||

transaction it can attack using some unwanted regular applied keys. Mathematically replay attack is, U_A→hash(□PW□_i)→U_B , User A send hash value to User B E_i←Sniff hash→U_A , Attacker sniffs hash value from User A E_i→replay hash , Attacker then replays hash over User B Mathematical proof for the prevention of replay attack, During registration of any new User on Server User needs to give his Identity and Password, on the basis of User's Identity and password hash values are generated and encrypted using elliptic curve and send to Server. T_1→□hash(ID□_i), User A calculates hash over his Identity T_2→hash(□ID□_i ||□PW□_i), User A calculates hash over concatenation of his Identity and password T→(T_1,T_2), tupple is created from both hash values E_i→E_T→S, tupple is then Encrypted using Elliptic Curve Cryptography and send to server □Attacker□_i←sniff E_i→U_A, Attacker sniff Encrypted value from User A □Attacker□_i→replay hash , Attacker then replays hash over User B Attacker when tries to attack with replay hash can't be applied on User B, since attack is done using some hash keys while the Data sends from User A is in Encrypted form which is hard to predict.

Sources	Similarity

SmallSEOTools

PLAGIARISM SCAN REPORT

Words	900	Date	August 16,2020
Characters	5958	Exclude Url	

2%	98%	1	39
Plagiarism	Unique	Plagiarized Sentences	Unique Sentences

Content Checked For Plagiarism

5.4.2 Identity Disclosure Attacks Here in this type of attack the attacker may uses the Identity of the friend who has Shares his Identity to Attacker. This type of attacks mainly observes in Online Social Networks. The Client when Shares or Disclose his Identity to the attacker, then the attacker may try to use the Identity of the fake Client and attack Victim. The Planned procedure implemented here prevents this type of attacks, since here if the Client Share his Identity to the attacker, then the attacker is unable to attack victim. Let us take an example Suppose Client 'S' has Identity 'IDi' which is shared with Attacker 'Ai' now when Attacker may want to send request to Victim it goes to Server for Verification and Authentication, when First Factor Applies Server asks for Attacker to Send Challenge Value. Attacker 'Ai' -> send request to Server Server acknowledges Attacker to send Challenge Value. Attacker 'A' sends any fake Challenge Value 'C' -> Server Server uses this C + (Secrete Password) -> Master Hash Value Server -> acknowledges Attacker to Send his Master Hash value. Now Attacker doesn't have Secrete Password so may use C+(fake password) -> master hash value and Send to Server. Server matched both Master Hash Values, it doesn't match and Attacker Denied. 5.4.3 Insider Attacks The planned procedure implemented is based on 2 Factor Authentication where the Authentication and verification of the user is independent of whether it is inside of the network or outside. If any Inside Attacker may tries to attack victim uses his public key he may be restricted at the second factor authentication where any user needs to use smart card for the authentication. T_1→□hash(ID□_i), User A calculates hash over his Identity T_2→hash(□ID□_i ||□PW□_i), User A calculates hash over concatenation of his Identity and password T→(T_1,T_2), tupple is created from both hash values E_i→E_T→S, tupple is then Encrypted using Elliptic Curve Cryptography and send to server □Attacker□_i→sniffs (□ID□_i) and □PW□_i, Attacker sniffs Identity and Password of User A Attacker when tries to attack Server using the Identity of User A then Server will refuse since User A is already registered and ask for Smart Cards based authentication. 5.4.4 Outsider Attacks The planned procedure implemented is based on 2 Factor Authentication where the Authentication and verification of the user is independent of whether it is inside of the network or outside. If any outside Attacker may tries to attack victim using public key of any user or any unwanted key he may be restricted at the second factor authentication where any user needs to use smart card for the authentication. T_1→□hash(ID□_i), User A calculates hash over his Identity T_2→hash(□ID□_i ||□PW□_i), User A calculates hash over concatenation of his Identity and password T→(T_1,T_2), tupple is created from both hash values E_i→E_T→S, tuple is then Encrypted using Elliptic Curve Cryptography and send to server □Attacker□_i→sniffs (□ID□_i) and □PW□_i, Attacker sniffs Identity and Password of User A Attacker when tries to attack User A for Identity and Password can't attack since the tuple is in Encrypted form and difficult to Decrypt. 5.4.5 Eavesdropping Attack The attacker could change a victim's contact data to trick the victim's contacts into sending sensitive data to the attacker, but the Attacker when tries to Authenticate at the Server he failed to authenticate himself. 5.4.6 Eurograbber Attack In this type of attack when Trojan's contaminate the User's mainframe and the occurrence witches communiqué with the series. In the Additional point aggressor recover the operator's mobile quantity and contaminate the mobile maneuver. In the next chapter the following time the operator fuels into the bank version, the aggressor recruits a transmission of reserves from the user's explanation to the "mule" explanation. In the last point Bank directs a Contract Agreement Quantity via SMS. Even though the Eurograbber Attack sniffs our First Factor Authentication but failed to authenticate during Second Factor, since it required Smart Cards for authentication and some computations needs to be performed by the User to issue these

Smart Cards. Table 5.1: Prevention of various attacks. Replay Attack Identity Disclosure Attack Insider Attack Outsider Attack Eavesdropping Identity Spoofing Password based Attack Man in the middle Attack Eurograbber Attack YES YES YES YES YES YES YES YES YES The table 5.2 shows the analysis of Storage Cost in bits during First Factor Authentication and overall time taken to generate the token. The Computation of Storage Cost in our scheme can be calculated as: N_t=hash(C_i)(1) N_s=hash(C_i)+hash(□PW□_i) (2) Where, N_t=No of bits in token C_i=Challenge value from User i N_s=No of bits in Secrete

N_s=hash(C_i)+hash(□PW□_i) (2) Where, N_t=No.of bits in token C_i=Challenge value from User i N_s=No.of bits in Secrete Value during First Factor Authentication □PW□_i=Password value of User i Table 5.2: First Factor Authentication No. of bits in token No. of bits in conceal value Time taken 32 bits 64 bits 11.538 sec The table 5.3 shows the analysis of Storage Cost in bits at the Smart Card and at the Server Side. The analysis done here is on the basis of R. Song et. al's and the proposed scheme implemented. The proposed scheme implemented takes less storage cost at the smart card and server side. The computation of storage cost in our scheme can be calculated as - T_s=□PA□_i+□PB□_i+□PC□_i+□PD□_i (1) T_s'=T_s+X_s+□ID□_i+□PW□_i (2) Where, T_s=Total Storage Cost at Smart Card □PA□_i=Hash(□ID□_i).xor.hash(X_s ||hash(□ID□_i)) □ID□_i=Identity of User i X_s=Secrete Key of Server □PB□_i=□PA□_i.xor.hash(□ID□_i ||□PW□_i) □PC□_i=hash(□PA□_i) □PD□_i=hash(□ID□_i ||□PW□_i).xor.hash(X_s) T_s'=Total Storage at Server □PW□_i=Password of User i

Sources	Similarity
YES YES YES YES, YES! 1 HOUR - YouTube Опубликовано: 3 мая 2020 г. yes yes yes yes, yes! https://www.youtube.com/watch?v=omVwIdP8GeY	3%

SmallSEOTools

PLAGIARISM SCAN REPORT

Words	660	Date	August 16,2020
Characters	4044	Exclude Url	

0%	100%	0	33
Plagiarism	Unique	Plagiarized Sentences	Unique Sentences

Content Checked For Plagiarism

5.5 ANALYSIS OF COMPUTATIONAL COST Total Computational Cost for First Factor Authentication The Planned procedure implemented here is based on the Concept of Two Factor Authentication to provide Security of Online Web Transactions. Hence during the Communication from Sender to Receiver or from Client to Server requires some Data to be Stored at the Client or at the Server Side. Let us consider for Single User 'Ui' Transaction on Web, so during First Factor Authentication User 'Ui' stores his Challenge Value 'Ci' and password 'Pi. Here in the First factor Authentication the Overall Computational Cost at the Client Side will be: C_Ui=C_Ci+C_Pi Where, C_Ui : Overall Computational Cost at the Client Side in bits. C_Ci : Overall Computational Cost of the Challenge Value at Client Side in bits. C_Pi : Overall Computational Cost of the Password at Client Side in bits. Similarly at the Server Side the Overall Computational Cost at the Server Side will be: C_Si=C_pi Where, C_Si : Overall Computational Cost at the Server Side in bits. C_Pi : Overall Computational Cost of the Password at Server Side in bits. Hence, overall Computational Cost for the First Factor Authentication will be C_1=C_Ui+C_Si Where, C_1 : Overall Computational Cost for the First Factor Authentication. Total Computational Cost for Second Factor Authentication Second Factor Authentication consists of Four Phases; hence overall computational cost at each stage of the algorithm is given as: During the registration phase when a new registration is send to Server and Server generates a Smart Card based on request, hence overall computational cost at the registration will be: C_ss=C_A+C_B+C_C+C_D Where, C_ss : Overall computational cost for smart card storage in bits. C_A : Overall computational cost for Parameter A in bits C_B : Overall computational cost for Parameter B in bits C_C : Overall computational cost for Parameter C in bits C_D : Overall computational cost for Parameter D in bits C=C_1+C_ss Where, C: Overall Computational Cost in bits. C_ss : Overall computational cost for smart card storage in bits. C_1 : Overall Computational Cost for the First Factor Authentication. The Table 5.4 is the analysis of the overall Computation cost by the planned procedure for number of Users. The Computational Cost for the No. of Users is less than the existing methodologies used for the Security prevention from various attacks. Table 5.4: Analysis of Computational Costs on bits No. of Users Computational Cost in bits 5 461 10 532 15 680 20 811 25 925 30 1051 35 1245 40 1377 45 1475 50 1543 The Figure 5.14 is the analysis of the overall Computation cost by the planned procedure for number of Users. The Computational Cost for the No. of Users is less than the existing methodologies used for the Security prevention from various attacks. 5.6 ANALYSIS OF COMPUTATIONAL TIME Computational time can be computed on the basis of communication time takes places at the First Factor and second factor Authentication. T=T_1+T_2 Where, T: Overall Communication Time in ms T1: Overall Communication Time for First Factor Authentication in ms. T2: Overall Communication Time for Second Factor Authentication in ms. However, Communication Time can be computed as the overall time algorithm will takes during sending and receiving of data from Client to Server or from Server to Client. The Table 5.5 is the analysis of the overall Communication time by the planned procedure for number of Users. The Communication Time for the No. of Users is less than the existing methodologies used for the Security prevention from various attacks. Table 5.5: Analysis of Communication Time in ms No. of Users Communication Time in ms 5 261 10 479 15 611 20 771 25 894 30 951 35 1050 40 1350 45 1528 50 1733 The Figure 5.15 is the analysis of the overall Communication time by the planned procedure for number of Users. The Communication Time for the No. of Users is less than the existing methodologies used for the Security prevention from various attacks.

Sources	Similarity

SmallSEOTools

PLAGIARISM SCAN REPORT

Words	419	Date	August 16,2020
Characters	3072	Exclude Url	

0%	100%	0	17
Plagiarism	Unique	Plagiarized Sentences	Unique Sentences

Content Checked For Plagiarism

6.1 CONCLUSION Security in various E-commerce Applications includes an efficient framework in Information Security especially in Data and Computer security and other Online transactions in E-commerce applications. Security in E-Commerce application plays an important role for the secure and scalable transaction which includes various dimensions such as security-integrity, Confidentiality, Non-repudiation, Privacy etc. Hence for the Security of Online Transactions in E-Commerce based application various Security algorithms are implemented. Although these Security algorithms are efficient and provides Security from attacks but Data Storage during the transactions and Computational time of the algorithms is also imperative. Hence an efficient algorithm is implemented which provides Security in Online E-Commerce transactions and also provides efficient Computational Cost and time. The planned procedure implemented here works on the framework of Authentication on Two Factor which provides Security from attacks especially in Online Web Transactions. The Methodology implemented works on two phases 1) Assigning the validity of the User by allocating a challenge value 2) Improved Smart Card based Authentication using Elliptic Curve based Encryption and Data Validation. The proposed technique implemented here prevents from numerous types of security attacks such as replay attack and identity disclosure attack or outsider attack and provides security from various dimensions such as security-integrity, Confidentiality, Non-repudiation, Privacy etc. The two factor verification that we proposed here takes low Computational Cost and Computational Time. The planned procedure when implemented on Applications such as E-Commerce based Online Transactions in Web Mining it provides Security from various attacks such as Replay Attacks, Identity Disclosure Attack, Insider Attack, Outsider Attack, Identity Disclosure Attack and Man-in the Middle Attack. The Methodology when applied on the quantity of customer / Users such as 5,10,15,20,25,30,35,40,45,50 it performs come computation at the Sender Side and Server Side and takes 461,532,680,811,925,1051,1245,1377,1475,1543 Computational Cost in bits and 261,479,611,771,894,951,1050,1350,1528,1733 Communication Time in milliseconds. 6.2 ADVANTAGES 1. Provides Security from security attacks in E-Commerce based Online Transactions. 2. Implementation of Authentication using Two Factorso that chances of fraud detection get minimized and Secrecy and Privacy is maintained. 3. The Methodology implemented takes less storage and Computational Cost from server side. 4. Provides less computational time. 5. The chief advantage of this explanation is that it delivers each user with the competence of collaborating steadily with other users in the system while only requiring it to remember a distinct password. This appears to be a more accurate situation in repetition than the one in which operators are probable to share multiple keywords, one for each gathering with which it may interconnect confidentially.

Sources	Similarity