

**TO DEVELOP A CLOUD BASED FRAMEWORK FOR SECURITY  
ASSESSMENT**

A Dissertation

Submitted

In Partial Fulfillment of the Requirements for  
The Degree of

**MASTER OF TECHNOLOGY**

In

Computer Science & Engineering

Submitted by:

**AZRA ZIA ANSARI**

Under the Supervision of:

**MRS. KAVITA AGARWAL**

(Associate Professor)



Department of Computer Science & Engineering  
Faculty of Engineering

**INTEGRAL UNIVERSITY, LUCKNOW, INDIA**  
**August, 2020**

## CERTIFICATE

This is to certify that **Ms. Azra Zia Ansari** (Enroll. No. 1400100659) has carried out the research work presented in the dissertation titled **“To Develop a Cloud Based Framework For Security Assessment”** submitted for partial fulfillment for the award of the **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 Grants 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 submission for the award of the aforesaid degree.

*Kavita Agarwal*

Mrs. Kavita Agarwal  
Dissertation Guide  
(Associate Professor)  
Department of CSE,  
Integral University, Lucknow

Dr. Mohammadi Akheela Khanum  
H.O.D.  
Department of CSE ,  
Integral University, Lucknow

Date: August 10, 2020

Place: Lucknow

## **DECLARATION**

I hereby declare that the dissertation titled **“To Develop a Cloud Based Framework For Security Assessment”** is an authentic record of the research work carried out by me under the supervision of Dr. Shish Ahmad, Department of Computer Science & Engineering , for the period from August,2019 to August, 2020 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 works of other researchers wherever their published works have been cited in the dissertation. I further certify that I have not willfully taken other's work, para, text, data, results, tables, figures etc. reported in the journals, books, magazines, reports, dissertations, theses, etc., or available at web-sites without their permission, and have not included those in this M.Tech dissertation citing as my own work.

Date: August 10, 2020



Azra Zia Ansari  
Enroll. No.1400100659

## **COPYRIGHT TRANSFER CERTIFICATE**

Title of the Dissertation: **To Develop a Cloud Based Framework For Security Assessment**

Candidate Name: **Azra Zia Ansari**

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 the M.Tech degree.

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



Azra Zia Ansari

## **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 my guide **Mrs. Kavita Agarwal, Associate Professor, Department of Computer Science and 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 Khanum (Associate Professor, Department Of Computer Science and Engineering)** and PG Program Coordinator **Dr. Faiyaz Ahamad, Assistant Professor, Department of Computer Science and 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 project work.

Date: August 10, 2020

Place: Lucknow

## **TABLE OF CONTENTS**

<b>Contents</b>	<b>Page No.</b>
Title Page	(i)
Certificate/s (Supervisor)	(ii)
Declaration	(iii)
Copyright Transfer Certificate	(iv)
Acknowledgment	(v)
Content of Table	(vi-vii)
List of Tables	(viii)
List of Figures	(ix)
Abstract	(x)
<b>Chapter 1- Introduction</b>	<b>1</b>
1.1 Introduction	2-5
1.2 History of Cloud Computing	5-8
1.3 Architecture of Cloud Computing	8-10
1.4 Characteristics of Cloud Computing	10-12
1.5 Types of Cloud Computing	13-14
1.6 Types of Cloud Service Model	14-16
1.7 Applications of Cloud Computing	17-19
1.8 Challenges of Cloud Computing	20-21
1.9 Limitation of Cloud Computing	21-23
1.10 Cloud security	24-26
1.11 Problem Definition	26
1.12 Proposed Goals	27
1.13 Methodology	27-29
1.14 Dissertation Outline	29-30
<b>Chapter-2 Literature Review</b>	<b>31</b>
2.1 Literature Review	32-42

2.2 Related work	42-45
2.3 Conclusion	45
<b>Chapter-3 Proposed Work</b>	46
3.1 Introduction	47
3.2 Security Parameter	47-49
3.3 Proposed model	49-50
3.4 Empirical Validation	50-55
3.5 AHP Methodology	55-57
<b>Chapter-4 Result Analysis and Discussion</b>	58
4.1 Introduction	59
4.2 Analysis and Discussion of Results	59-65
<b>Chapter-6 Conclusion and Future Work</b>	67
6.1 Conclusion	68-69
6.2 Future Work	69
<b>References</b>	70-73
<b>Appendix</b>	
<b>Plagiarism Check Report</b>	74
<b>Publication from This Work</b>	82

## **LIST OF TABLES**

Table 2.1: Literature Review Summary	38
Table 2.2: Contribution table by Experts with Year	44
Table 3.1 Preference of Security Criteria	49
Table 3.2 Intensity of preference between different criteria	50
Table 3.3 Intensity Chart	51
Table 3.1 Full matrix based on paired comparisons	52
Table 3.5 Original score	52
Table 3.6 Authorization score	53
Table 3.7 Authentication score	53
Table 3.8 Non repudiation score	58
Table 4.1 Pair Wise comparison	60
Table 4.2 Original score	63
Table 4.3 Weighted score	63
Table 4.4 Final Weight score	64



## **LIST OF FIGURES**

Figure 1.1: CLOUD COMPUTING	4
Figure 1.2: different technologies cloud cover	5
Figure 1.3 : HISTORY OF CLOUD	8
Figure 1.4: ARCHITECTURE OF CLOUD COMPUTING	9
Figure 1.5 Types of Cloud	14
Fig.1.6. Infrastructure as a Service	15
Fig.1.7. Platform as a Service	16
Fig.1.8. Software as a Service	17
Figure 1.9: Process of Research Methodology	28
Figure 3.1 Cloud Security Model	49
Figure 4.1 Comparison of original score	65
Figure 4.2 Comparison of Weighted score	66
Figure 2.3 Comparison of Final score	66

## **ABSTRACT**

Cloud computing has emerged as a latest generation technology which host and deliver services by the use of internet. It is also a versatile technology that can support a broad spectrum of application. Cloud has many known service providers such as Amazon Web Service (AWS), IBM Garage, Google's application, Microsoft Azure etc. These cloud service providers provide users with developing applications in cloud environment and to access them from anywhere.

Cloud computing major role in providing security to the data which is transmitted to the remote server over internet. It faces critical challenge in cloud computing which includes user's secret data loss, data leakage and disclosing of the personal data .There possibility of the server breakdown that has been looked in the recent times, so various issues that have to be dealt with respect to security in cloud computing. Cloud has single security architecture but have many customers with demands. Now a day's cloud computing have become in demand and are used in various fields such as health care, education, business, and many more domains because of its property of low cost, high availability and scalability. As being an emerging field customers use this according to their convenience so privacy and security is an important issue in cloud computing. In this paper we will introduce cloud computing and study about the security issues and come up with a framework which can effectively solve these security issues.

There are various research work carried out in past has done some major contribution, but still the problems of security is still unsolved in many cases. The proposed work introduces techniques that are considered as major contribution in the research toward security in cloud that is based on cloud environment. The main object of this thesis work is to propose a novel, secure communication and security in a cloud based environment

## **CHAPTER: 1**

### **INTRODUCTION**

## **1.1 INTRODUCTION OF CLOUD COMPUTING**

The term cloud assign to the network or an internet. It is a technology that uses remote servers on the internet for storing and accessing data and programs over the internet instead of your computer's hard drive.

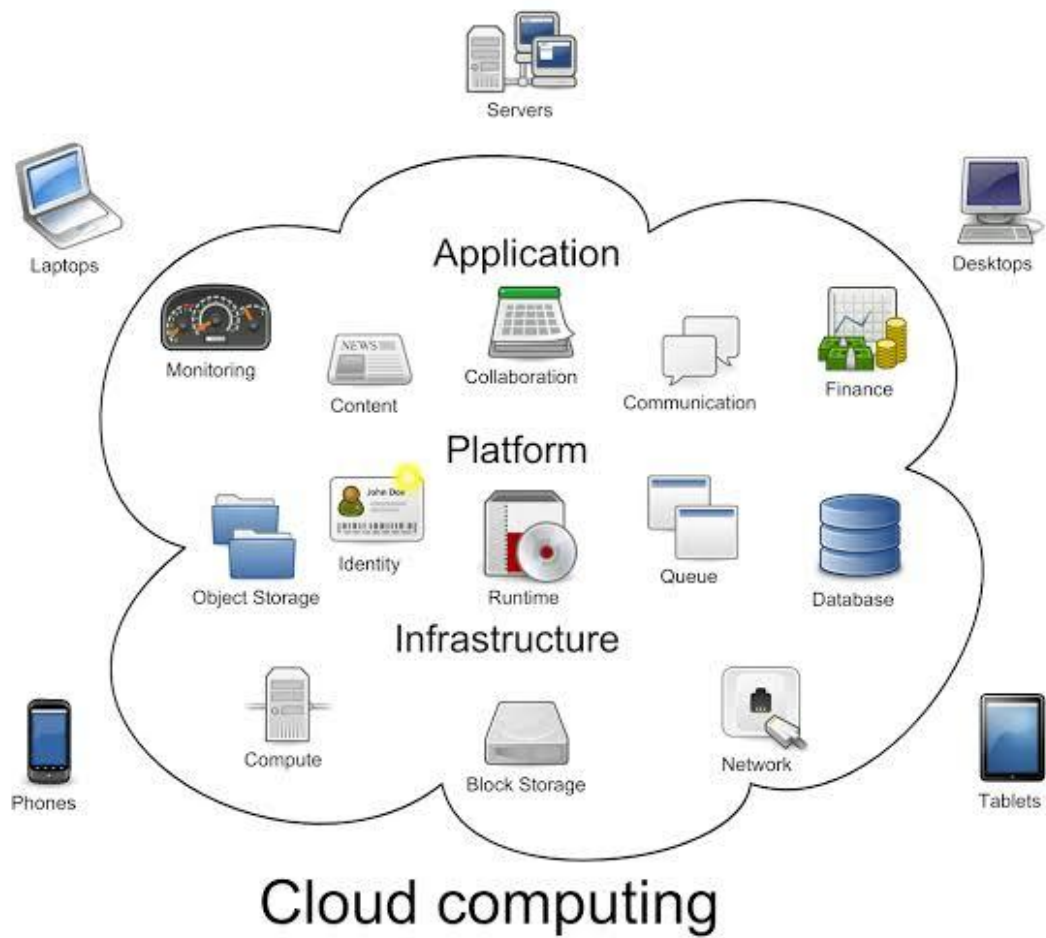
Cloud computing is a popular solution to provide cheap and easy access to external information and technological resources. An increasing number of organization benefit from the cloud computing to host their applications. Cloud computing has become an emerging technique due to its on demand service and scalability feature.

Most usage of cloud today is in computation intensive applications big data and data storage.

Cloud computing technology has to face new challenges as well as requires the new security issues. Security is on the key challenges which has become the talk of the town these days. In previous year, the cloud services have had many security accident.

For example, in March 2009 Google leaked a large number of documents of the users same problem was faced by facebook in 2019 about the leak of the data of the users. the following operations that can be done using cloud computing are:

- Developing new applications and services
- Storage, back up, and recovery of data
- Hosting blogs and websites
- Delivery of software on demand
- Analysis of data
- Streaming videos and audios



**Figure 1.1: CLOUD COMPUTING**

However, cloud services are used by many technologies in the present time. There are some technologies using the cloud service such as mobile, computer, facebook, dropbox, gmail, Netflix, linkedIn etc



**Figure 1.2: different technologies cloud cover**

## **1.2 HISTORY OF CLOUD COMPUTING**

At the beginning technological era, the mainframe and terminal application the Client-Server architecture was also popular. The mainframe connected both types of resources and served them to a small client-terminal because at that time storing of resources was very costly.

Cloud computing is one the most innovative and excellent technology of our time for storing of data.

Following is the history of Cloud computing

## **IN 1969**

The idea of an “Intergalactic Computer Network” or “Galactic Network” (a computer networking concept similar to today’s Internet) was introduced by J.C.R. Licklider, who has developed ARPANET (Advanced Research Projects Agency Network). His vision was to be able to access programs and data at any site, from anywhere

## **IN 1970**

Using virtualization software like VMware. It became possible to run more than one Operating System parallel in an isolated environment.

It was possible to run a completely different Computer that is a virtual machine inside a different Operating System.

## **IN 1997**

The first definition of the term “Cloud Computing” seems was given by Prof. Ramnath Chellappa in Dallas in 1997 – “A computing paradigm where the boundaries of computing will be determined by economic rationale rather than technical limits alone.”

## **IN 1999**

The arrival of Salesforce.com in 1999 pioneered the concept of delivering enterprise applications by simple website. To deliver applications over the Internet the services firm covered the way for both specialist and mainstream software firms.



### **IN 2003**

The first public release of Xen, which was the release of first Virtual Machine Monitor (VMM) also called as a hypervisor, a software system that allows the execution of multiple virtual guest operating systems on a single machine.

### **IN 2006**

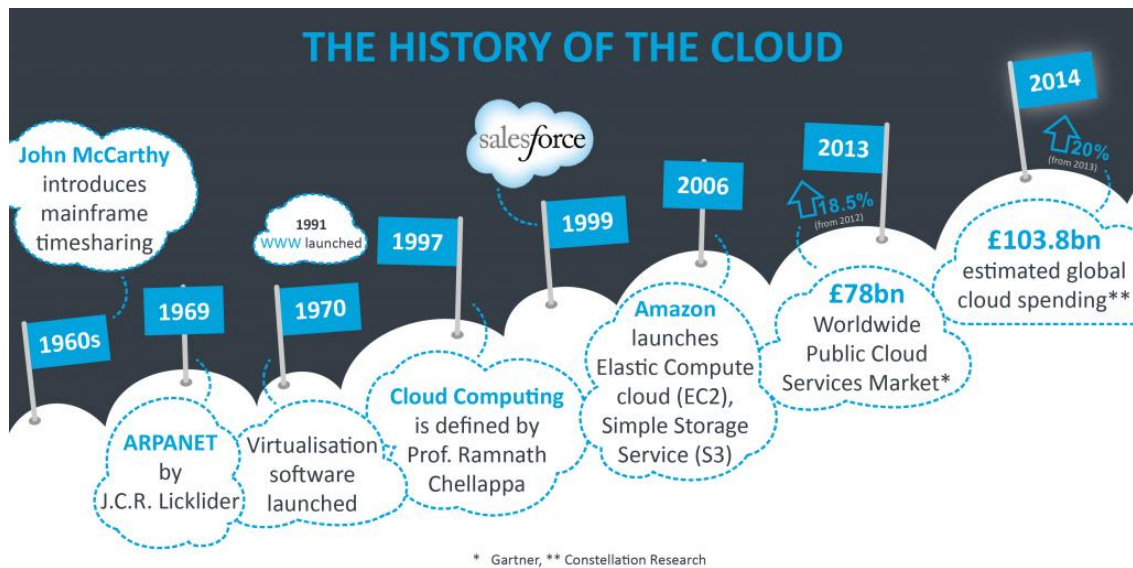
In 2006, Amazon expanded its cloud services on which first was its Elastic Compute cloud (EC2), which allowed people run their own application and access computers on the cloud, all on the cloud. Amazon then brought Simple Storage Service (S3). This S3 introduced the pay-as-you-go model to both users and the industry and it is now used as standard.

### **IN 2013**

The Worldwide Public Cloud Services Market totalled £78bn, up 19.5 per cent on 2012, with IaaS (infrastructure-as-a-service) was the fastest growing market service in cloud.

### **IN 2014**

IN 2014, global business spending for IaaS related to the cloud will reach an estimated £103.8bn, up 21% from the amount spent in 2013 (Constellation Research).



**Figure 1.3 : HISTORY OF CLOUD**

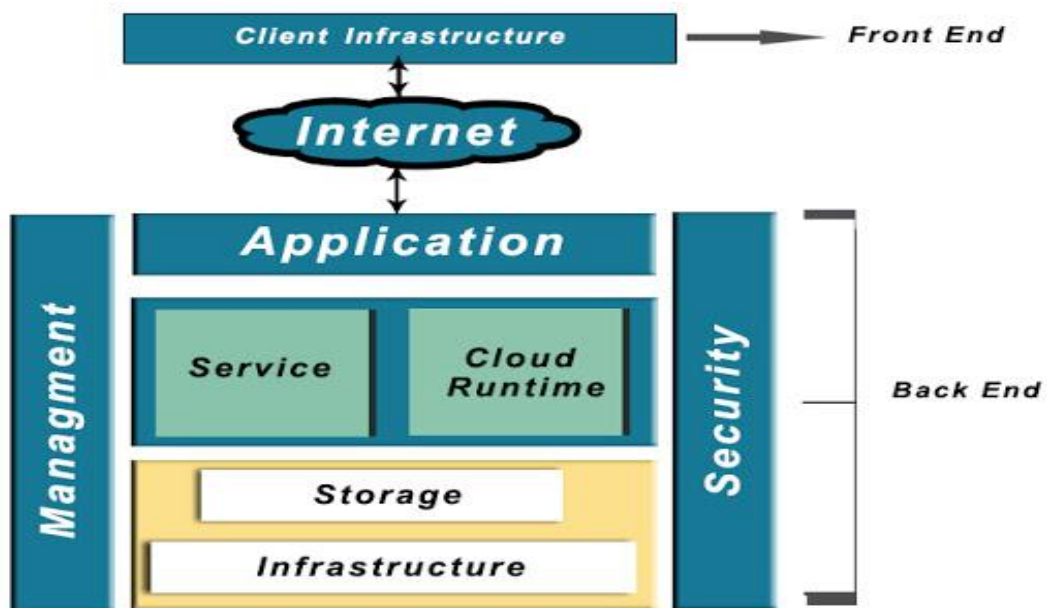
### **1.3 ARCHITECTURE CLOUD COMPUTING**

A Cloud computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer. Cloud computing has emerged as a latest generation technology which host and deliver services by the use of internet. It is also a versatile technology that can support a broad spectrum of application. Cloud has many known service providers such as Amazon IBM, Google’s application, Microsoft Azure etc. These cloud service providers provide users with developing applications in cloud environment and to access them from anywhere. They also have a major role in providing security to the data which is transmitted to the remote server over internet.

Security is an important and a critical challenge in cloud computing which includes user’s loss of data, leakage of data and disclosing of the personal data and also the

possibility of server breakdown cannot be denied, in the recent times, so we have various issues which need to be dealt with in security of cloud computing.

Cloud has single security architecture but have many customers with demands. Now a day's cloud computing have become in demand and are used in various fields such as health care, education, business, and many more domains because of its property of low cost, high availability and scalability. As being an emerging field customers use this according to their convenience so privacy and security is an important issue in cloud computing.



**Figure 1.4: ARCHITECTURE OF CLOUD COMPUTING**

## **1.4 CHARACTERISTICS OF CLOUD**

Following are the characteristics of Cloud Computing:

- Great Availability of Resources
- On-demand Self-service
- Easy Maintenance
- Large Network Access
- Availability
- Automatic System
- Economical
- Security
- Pay as you go

### **Great Availability of Resources**

This service is made to serve multiple customers and this is done with the help of the multi-tenant model. There are many physical and virtual resources provided which can modify as per the customer's demand. We can say that the customer doesn't have the knowledge that where the data is stored and even they don't have the control over it.

### **On-Demand Self-Service**

It is one of the important and valuable features of cloud computing as the user can continuously monitor the server uptime, capabilities, and allotted network storage. With this feature, the user can also monitor the computing capabilities.

### **Easy Maintenance**

The servers are easily maintained and the downtime is very low; in some cases, there is no downtime. The cloud computing comes up with an update every time by gradually making it better. The updates are more compatible with the devices and perform faster than older ones along with the bugs which are fixed.

### **Large Network Access**

The user can access the data of the cloud or upload the data to the cloud from anywhere just with the help of a device and an internet connection. These capabilities are available all over the network and accessed with the help of internet.

### **Availability**

The capabilities of the cloud can be modified as needed and can extend a lot. It

analyzes the storage usage and allows the user to buy extra storage if needed for a very small amount. This service is available anytime and can be accessed from anywhere.

### **Automation**

Cloud computing automatically analyzes the data needed and supports a metering capability at some level of services. This usage can monitor, control, and report, providing transparency for the host as well as the customer.

### **Economical**

It is the one-time investment as the company (host) has to buy the storage and a small part of it can provide to the many companies which save the host from monthly or yearly costs only the amount which spends on the basic maintenance and few more expenses.

### **Security**

This is one of the best features of cloud computing. It creates a snapshot of the data stored so that the data may not get lost even if one of the server damages.

The data stores within the storage devices which cannot hack and utilize by any other person. The storage service is quick and reliable which can access from anywhere just with the help of a device and internet connection.

### **Pay-as-You-Go**

In cloud computing, the user has to pay only for the service or the space they have utilized. There is no hidden or extra charge which is to be paid. The service is economical and most of the time some space allows for free.

## **1.5 TYPES OF CLOUD COMPUTING**

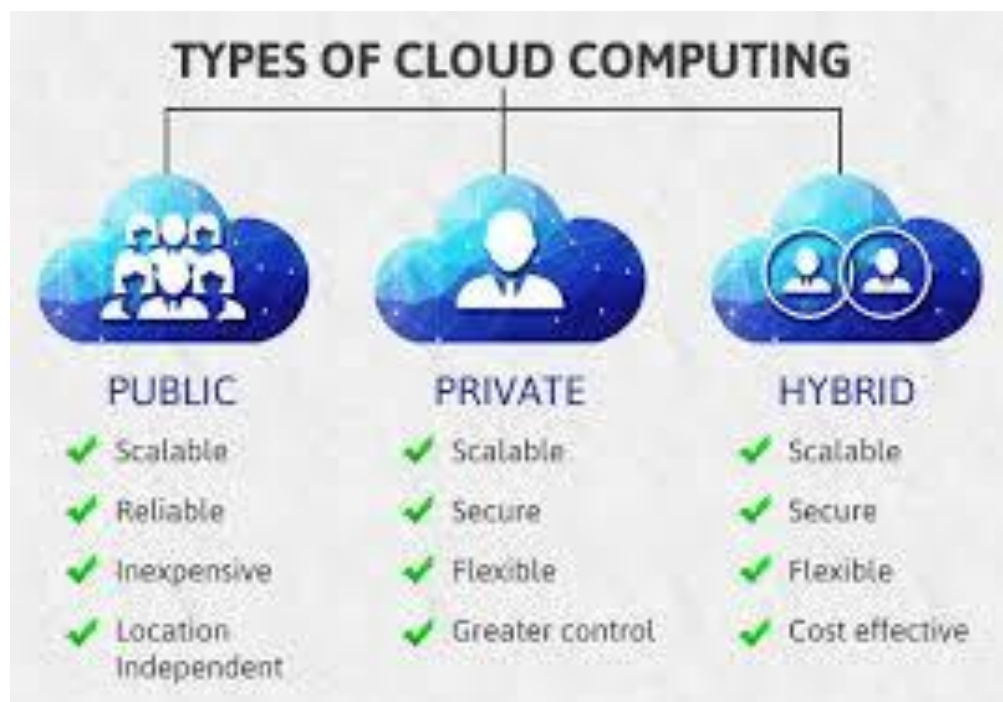
According to business needs there are four different cloud models:

**Private Cloud:** It is the cloud which is provided for use of any one particular organisation or company. This method is mostly used for intra-business purpose. Where the cloud deployed in the organisation or company are allowed governed, owned and operated by the same company or organisation.

**Community Cloud:** It is the cloud model which is provided to the community.

**Public Cloud:** This type of cloud is usually for B2C that is business to Consumer communication. Here the cloud is owned, governed and operated by business organization or government.

**Hybrid Cloud:** This type of cloud can be used for both type of communications B2B that is Business to Business or B2C that is Business to Consumer.



**Figure 1.5 Types of Cloud**



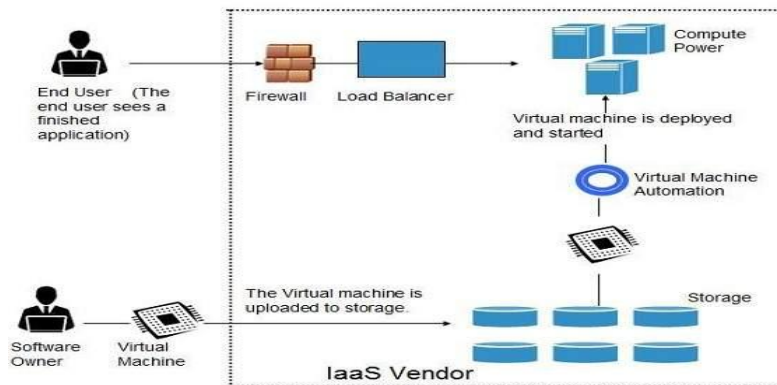
## 1.6 TYPES OF CLOUD SERVICE MODEL

### Infrastructure as a service:

Infrastructure-as-a-Service provides access to fundamental resources such as physical machines, virtual machines, virtual storage, etc.

The IAAS offers many other resources:

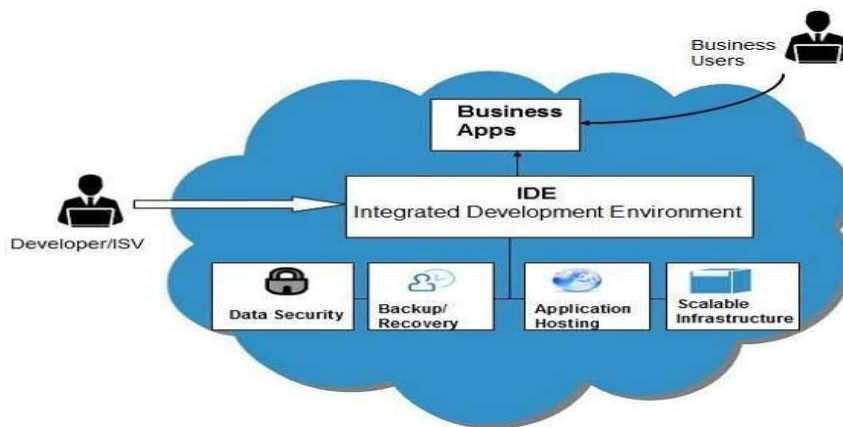
- Virtual machine disk storage
- Virtual local area network (VLANs)
- Load balancers
- IP addresses
- Software bundles



**Fig.1.6. Infrastructure as a Service**

### Platform as a Service:

It offers development and deployment tools which are required to develop an application. PAAS helps non-developers to create web applications with the feature point-and-click tools. Most highlighted PaaS offering vendors examples are App Engine of Google and Force.com. if a Developer wants to create web-based applications they can log in to these websites and use API given..



**Fig.1.7. Platform as a Service**

**Software as a Service:**

Software-as-a-Service (SaaS) model provides the software for the service for end users. This software is accessible by the internet and is deployed on the host. There are many SaaS applications which are been listed below:

- Billing and invoicing system
- Customer Relationship Management (CRM) applications<sup>3</sup>.
- Help desk applications<sup>4</sup>.
- Human Resource (HR) solution.



**Fig.1.8. Software as a Service**

## **1.7 APPLICATION OF CLOUD COMPUTING**

### **1. Art Application**

Cloud computing offers many applications which are used for designing images, cards or booklets. Some widely used cloud art applications are listed below:

i. Moo

ii. Vistaprint

iii. Adobe Creative Cloud

## 2. Business Applications

Business applications are based on cloud service providers. Today, every organization wants to grow in the field of cloud in business. It also makes the business applications to be available 24\*7 to the users.

There are the following business applications of cloud computing -

i. MailChimp

ii. Salesforce

iii. Chatter

iv. Bitrix24

v. Paypal

vi. Slack

vii. Quickbooks

## 3. Data Storage and Backup Applications

In Cloud computing we can store information's on cloud of all kind and type like data,files, images, audios, and videos and can be used via internet. As the cloud provider also makes backup of the files for recovery or while loss of data and is also responsible for providing security.

Various types of data storage and backup applications in the cloud are as follows -

- i. Box.com
- ii. Mozy
- iii. Joukuu
- iv. Google G Suite

#### 4. Education Applications

Cloud computing has become very highlighted in education sector. For learning cloud various types of cloud portals, distance learning programs and short courses are being provided for the students and the people who want to learn about cloud. There are many advantage of using cloud in education system like providing virtual classroom, accessibility is easy, data storage is secured, scalability, students can reach at good heights in the career, and least requirements of hardware for the applications.

Education applications offered by the cloud are:

- i. Google Apps for Education
- ii. Chromebooks for Education
- iii. Tablets with Google Play for Education

#### iv. AWS in Education

### 5. Entertainment Applications

Entertainment industries when have to interact with the audience uses a multi-cloud strategy. Cloud computing has various entertainment applications such as:

#### i. Online games

#### ii. Video Conferencing Apps

### 6. Management Applications

Cloud computing has many cloud management tools which help to manage cloud activities that are resource deployment, data integrity and data recovery. They also provide administrative control over the platforms, applications, and infrastructure.

Some important management applications are -

#### i. Toggl

#### ii. Evernote

#### iii. Outright

#### iv. GoToMeeting

## 7. Social Applications

Social networking sites like facebook, twitter, linkedin, etc. In which large no. Of users are connected is only possible because of cloud computing because of which we can store data at large scale.

Following are the cloud based social applications –

i. Facebook

ii. Twitter

iii. Yammer

iv. LinkedIn

## **1.8 CHALLENGES OF CLOUD COMPUTING**

There are many challenges to be focus in cloud computing even after so good features it still have challenges for the security and data. These challenges are

- Security and Privacy
- Portability
- Interoperability

- Computing Performance
- Reliability and Availability

**Security and Privacy:** Security and Privacy of information is the main challenge to be focus on cloud computing. These issues can be removed by encryption, security hardware and security applications.

**Portability:** In cloud computing it is necessary that cloud provided can work on all type of devices and easily accessible. There must not be vendor lock-in. However, this is not possible every developer makes use of their preferable platform for the process.

**Interoperability:** It means the application on one platform should be able to use the information and services from the other platforms. It is done by the use of web services, which is complex.

**Computing Performance:** applications on cloud require very high network bandwidth, which means is cost is high. Low bandwidth makes performace of computing very slow and does not meet desired goal.

**Reliability and Availability:** most of the businesses are now becoming dependent on services provided by third-party which has made necessary for the cloud system to be more reliable and robust.

## **1.7 LIMITATION OF CLOUD COMPUTING**

There are a lot of features of cloud computing. The area of applications for cloud is varied, but there are many limitations in cloud computing. These are

### **Performance**

In a cloud environment, application is running on the server which provides resources



to other businesses. The performance of shared resource can be attack by any greedy behavior or DDOS attack on tenant.

### **Technical Issues**

Cloud technology is always susceptible to a dimout and other technical issues.

Even, despite maintaining standards of maintenance the cloud service provider companies have to face this type of problem.

.

### **Security Threat in the Cloud**

In the Cloud another problem while working with cloud computing services is security risk. Before adopting cloud technology, we should be well aware of the fact that they will be sharing all company's sensitive information to a third-party cloud computing service provider. Hackers may be access this information.

### **Downtime**

Downtime can also be considered while working with cloud computing. That's because cloud provider may face power loss, low connectivity of internet, maintenance service, etc.

### **Internet Connectivity**

Good Internet connectivity is necessary in cloud computing. We wouldn't access cloud without an internet connection. Moreover, we don't have any other way to collect data from the cloud.

### **Lower Bandwidth**

Many cloud storage service providers limit bandwidth usage for their users. So, in case if your organization big then given allowance, the additional charges could be costly.

### **Lacks of Support**

Support Cloud Computing companies fail to provide good support to the customers. They want their user to depend on FAQs or online help, which can be a big problem for non-technical persons.

## **1.8 CLOUD SECURITY**

A Cloud security is the protection of data stored online via cloud computing platforms from theft, leakage, and deletion.

Cloud security can be provided by following method include firewalls, penetration testing, obfuscation, tokenization, virtual private networks (VPN), and avoiding public internet connections. Cloud security is said to be like cybersecurity.

Cloud security refers to measures taken to protect data stored online by cloud services providers. Cloud computing is the considered to be the delivery of different services through the Internet, which includes data storage, servers, databases, networking, and software. To protect this data measure which is taken is known as two-factor authorization (2FA), the use of VPNs, security tokens, data encryption, and firewall services and many others.

For cloud storage providers cloud security is the main concern. They must follow certain regulatory requirements for storing sensitive data such as credit card numbers and health information and also keep in mind about the satisfaction of the customer.

## **Confidentiality**

Confidential information must only be accessed, used, copied, or disclosed by only authorized users which proper passwords safety.

Confidentiality occurs only if an unauthorized persons or any information which has be hidden is been disclosed that is not allowed. To prevent this leak of data information like a credit card number from eavesdroppers for that the transmission must be encrypted. In addition, to prevent unauthorized access the number must be protected wherever it will be processed or stored (e.g., databases).

## **Integrity**

Integrity means that data information should not be modified by any unauthorized person i.e. cannot be altered or tampered. It ensures that messages received or send are not unauthorized modified by any hacker. The hash value of a file or the message authentication code (MAC) of a message would change, if information has been changed, too. Thus, a modification should be known when comparing the current and the original information.

## **Availability**

Availability assumes that information systems and services are available in all the operating system and devices. It could be also considered as the degree to which a system is available for work.

## **Authentication**

Authentication is the process of verifying the credentials of an entity trying to access a protected resource. Authentication must be done in a secure, trustworthy, and

manageable manner. For accounts that require higher levels of security, multiple factor authentications may be required.

### **Non-repudiation**

It is always challenging to ensure true non-repudiation, outsourcing IAM to a SaaS provider may make this even more difficult due to the trust boundaries between provider and subscriber

### **Authorization**

Authorization management in the cloud should ensure that users have appropriate rights to access cloud as well as enterprise managed resources. Both policy definition and enforcement functions need to be available.

## **1.9 PROBLEM DEFINITION**

In recent years cloud computing have received wonderful consideration because of their storing and accessing of data and computing services over the internet. Different companies or organization are using this technology for storing their data in the cloud.

There are several security issues for storing the data in cloud server. To developed a cloud based framework for security assessment.

## **1.10 PROPOSED GOALS**

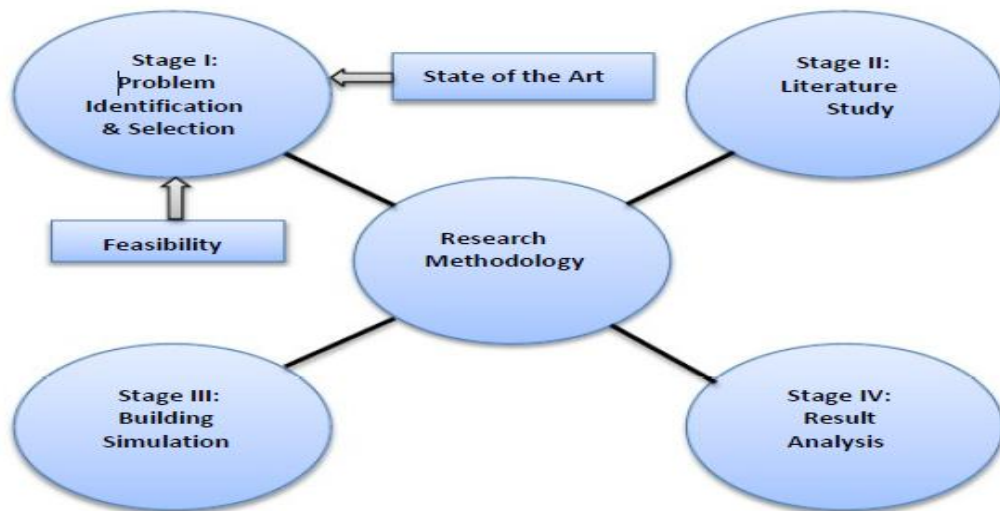
The main objective of Designs secures model which detects the malicious security parameter in cloud computing.

1. This dissertation aims at detect the security issues in cloud.
2. Identify the malicious security issues.
3. Verify the parameter that it is the intruder or malicious security issues.

## **1.11 METHODOLOGY**

A Research process consists of series of procedures or steps necessary to successfully carry out research and the preferred sequencing of these steps to produce new knowledge, or to offer a new manner of accepting present knowledge.

We have practical a quantitative approach towards the study. In distinct phases we have designed this work, each stage having its own importance. We started our work by a state of the art. After identification of the problem, we have done a literature survey in a detailed, focusing on the security issues of cloud computing. This literature review was followed by a simulation modeling. The results were gathered, analyzed and conclusions were drawn on the basis of the results obtained from the simulation.



**Figure 1.11: Process of Research Methodology**

### **STAGE I: PROBLEM IDENTIFICATION AND DATA SELECTION**

The selection of the proper problem and its identification at the outset is the most important phase. After a detailed study on the different areas of the cloud computing, we arrived at a conclusion on the identified problem. We aimed at focusing on security attacks in cloud for storing the data on the network.

### **STAGE II: LITERATURE STUDY**

A review of the state of the art was made after the identification of the problem. With expertise on cloud and its security issues, the most important thing is to understand its

basics. A literature survey was conducted in order to gain the solid background for the analysis of various security attacks. Different simulation tools and their functionalities were studied. In fact, this literature study enabled us to understand in detail the cloud computing and the security parameter involved in cloud i.e. authentication, authorization and non repudiation.

### **STAGE III: BUILDING SIMULATION**

In order to analyze the problem, we simulated the problem with a model of the system on AHP simulation tool. We simulated and developed the discrete-event simulation, where we created different scenarios according to the requirements of the problems. These scenarios were simulated by introducing malicious security issues in the simulated network. The results were gathered and analyzed in the fourth step of research design.

### **STAGE IV: RESULT ANALYSIS**

The most important stage is the last stage. we compare the weight score before and after pair comparison using AHP tool . All the results obtained from simulation AHP tool were analyzed.

## **1.14 DISSERTATION OUTLINE**

The rest of this document is organized as follows.

## **Chapter 2**

In this chapter I reviewed various national and international journals and publications to identify the real problem statement for doing appropriate research to detect security problems in cloud environment.

## **Chapter 3**

In this chapter, our proposed work discusses and explained in detail for detection and verification security parameter in cloud computing using AHP methodology.

## **Chapter 4**

In this chapter the metrics that were used to measure the performance of proposed work along with diagrams that illustrate the security measurements, the implementation details and results of the detection mechanism is discussed. In order to give more clear view of the implementation details involved part results are presented as graphs.

## **Chapter 5**

In this chapter conclusion and some of the future scopes discussed of this work.



## **CHAPTER: 2**

### **LITERATURE REVIEW**

## **2.1 LITERATURE REVIEW**

1. In 2019, Aakriti Sharma et al published an article Authentication Issues and Techniques in Cloud Computing Security: A Review, in this paper author discuss the methods of user's authentication and challenges faced in cloud computing. And discuss about the security issues in cloud computing and make an observation on user authentication techniques.
2. In 2019, Dhurate Hyseni et al published an article The Proposed Model to Increase Security of Sensitive Data in Cloud Computing in this they proposed a security model in cloud working on different conditions, especially for those environment that work is based on sensitive data and those companies that still hesitates to deploy in cloud.
3. In2019, V. Carchiolo et al published an article Authentication and Authorization Issues in Mobile Computing: A Case Study in this paper author discuss issues in mobile cloud computing and presented the solution of authorization and authentication issues in mobile cloud computing. By applied within the STMicroelectronics IC manufacture plants. It's also improve by introducing strong mechanism as trustworthiness.
4. In 2019, Bogdan Cosmin Chifor et al published an article Security Oriented Framework for Internet of thing Smart Home application in this paper author present a security framework for smart Home. They proposed a secure cloud which acts as proxy between the IOT devices and third party functional cloud along with a

- key escrow scheme which enables a smartphone based authorization mechanism. And solution is an extension for the EAP-NOOB security scheme acting as a command authorization.
5. In 2018, Adnaan Arbaaz Ahmed et al published an article Study of Security Issues and Research Challenges in this paper they discuss various models of cloud computing, security issues and research challenges in cloud environment. In this they also discuss about the multi –tenancy which is also a major issue in cloud computing security.
  6. In 2017, Huma Farooq published an article A Review on cloud computing Security Using Authentication Techniques In this paper author discuss about the security issues resolve by using authentication techniques such as username and password, MTM, multifactor, PKI, Single sign On and biometric authentication.
  7. In 2017, Gururaj Ramchadra et al published an article A Comprehensive Survey on Security in Cloud Computing, in this paper author summarizes a number of review articles on security threats in cloud computing and the preventive methods. Secondly to understand the cloud components security issues and risk along with emerging solution.
  8. In 2016, Priya Anand et al published an article Threat Assessment in the Cloud Environment – A Quantitative Approach for Security Pattern Selection, in this paper author provide a novel methodology to select a set of security patterns for

- securing a cloud software. This methodology could aid a security expert to assess the current vulnerability condition and prioritize by also including client's security requirement in cloud environment
9. In 2015, Ali Gholami et al published an article Security and Privacy of Sensitive Data in Cloud Computing: A Survey on Recent Developments, in this paper the author have made an overview of research on security and privacy of sensitive data in cloud computing environment. They have identify new development in the area of resource control, physical hardware, and cloud services management layer of a cloud provider.
  10. In 2015, Sunil Kumar et al published an article Data Security Framework for Cloud Computing, in this paper the author proposed the framework which the authenticate of the user who want to access the data, which is available on the cloud server.
  11. In 2015, Dr. Ambika Pawar published an article Security and Privacy in Cloud Computing: A Survey, in this paper the author survey on the different environment. Secondly there are many researcher which proposed the method to tackles issues by using different approaches. Which helps to minimize the problem over the security and privacy in cloud computing
  12. In 2013, Zhifeng Xiao et al published an article Security and Privacy in Cloud Computing, in this articles the author have made study on various types of security and privacy of cloud computing. In this paper author have identified five most

representative security and privacy attributes (i.e. Confidentiality, Integrity, Availability, Accountability, and privacy preservability).

13. In 2013, Kashif Munir et al published an article Framework for Security Cloud Computing, in this paper the author proposed a framework which identified the security challenges in the cloud computing. Identified security requirement, attacks, threats, concerns associated to the deployment of the cloud computing.
14. In 2012, Abdullah Abuhussein et al published an article Evaluating Security and Privacy in Cloud Computing Services: A Stakeholder's Perspective, in this article author has presented the aim of identify and categorize the attributes which highlight the security and privacy. Secondly this paper present how one can use these attributes for assessing and comparing potential cloud computing services both from a provider and a consumer stand point.
15. In 2012, Akhil Behl et al published an article An Analysis of Cloud Computing Security Issues in this article Cloud provides various facility and benefits but still it has some issues regarding safe access and storage of data. Several issues are there related to cloud security as: vendor lock-in, multi-tenancy, loss of control, service disruption, data loss etc. are some of the research problems in cloud computing.
16. In 2012, Hong Zhao et al published an article Data Security and Privacy Protection Issues in Cloud Computing, in this paper it presents a concise but all around

analysis on data security and privacy protection issues associated with cloud computing across all stages of data life cycle.

17. In 2012, Eman M.Mohamed et al published an article Enhanced Data Security Model for Cloud Computing, in this paper author identifies the basic problem of cloud computing data security. They present the data security model on the study computing based on the study of cloud architecture to improve for cloud computing.

18. In 2012, J.Srinivas et al published an article cloud basic computing, in this paper author explore the different concept involved in cloud computing. Leveraging there experiences on various cloud they examine cloud from technical and service aspect. Show some of opportunities in cloud computing and underlining the importance of clouds computing. Showing why this technology must succeed. Discuss about some of the issues that area should deal with.

19. In 2012, Youssef A.E. publish an article Exploring Cloud Computing Services and Applications, in this paper author explore the concept of cloud has emerged in two broad perspectives – renting of infrastructure on cloud, or renting any utility on cloud. Where the former one deals with the hardware and software utilization, the latter one is restricted to availing various utilities and not the hardware from the cloud service and infrastructure providers.

20. In 2011, Xiaowei Ysn et al publish an article The Research and Design of Cloud Computing Security Framework, in this paper they have presented the security problems introduces cloud computing security situation and also give the security framework of cloud computing.
  
21. In 2009, B. R. Kandukuri et al published an article Cloud Security Issues, in this paper they focus on the security issues in cloud computing. The Cloud Security Alliance is a nonprofit organization formed to promote the use of best practices for giving security affirmation inside Cloud Computing, and give instruction on the employments of Cloud Computing to help secure every single type of computing. The Open Security Architecture is another organization focusing on security issues.
  
22. In 2008, L. Wang et al published an article Cloud Computing: A Perspective Study in this paper they discuss while providing data security for customers' personal or business related data by only applying the simple strategic policies or specifically applying alone technical security is insufficient to deal with all type of security issues to maintain the high quality of service.

**Table 2.1 Literature Review Summary**

S.No.	Year	Title	Author	Description
1	2019	Authentication Issues and Techniques in cloud computing security : A Review	Aakriti Sharma et al	In this paper author discuss about the security issues in cloud computing and the most important issues raised in this cloud is authentication.  Discuss about the techniques that observe on user authentication techniques.
2	2019	Authentication and Authorization Issues in mobile computing : A case study	V. Carchiolo et al	In this paper author discuss issues in mobile cloud computing and presented the solution of authorization and authentication issues in mobile cloud computing.  By applied within the STMicroelectronics IC manufacture plants.  It's also improve by



				introducing strong mechanism as trustworthiness.
3	2019	Security Oriented Framework for Internet of thing Smart Home application	Bogdan Cosmin Chifor et al	In this paper author present a security framework for smart Home. They proposed a secure cloud which acts as proxy between the IOT devices and third party functional cloud along with a key escrow scheme which enables a smartphone based authorization mechanism. And solution is an extension for the EAP-NOOB security scheme acting as a command authorization.
4	2017	A Review on cloud computing Security Using Authentication Techniques	Huma Farooq	In this paper author discuss about the security issues resolve by using authentication techniques such as username and password, MTM, multifactor, PKI, Single

				sign On and biometric authentication.
5	2015	Security and Privacy in cloud computing: A Survey	Mahesh U. Shankarwar et al	<p>In this paper author discuss about the perception of different threats in cloud computing environment with respected to security and Privacy of user's sensitive data in cloud.</p> <p>In this paper author discussed about the advantages and limitations of existing method to completely solve security and privacy issues.</p>
6	2015	Data Security Framework for Secure cloud computing	Sunil Kumar et al	<p>In this paper author proposed</p> <p>A security framework for cloud i.e. able to identify the security attacks, threat and risk in the cloud deployment. And Analyse the security issues of Cloud Service provider in the</p>

				domain of integrity, authenticity and availability. Discuss its solution of cloud security.
7	2013	Security and Privacy in Cloud Computing	Zhifeng Xiao et al.	In this paper the author studies about the security and privacy issues in cloud computing based on an attributes driven methodology. The attributes which are identified the most representative security/privacy are confidentiality, integrated by various attacks. Also discuss about the defend strategies and suggestion to solve the issues.
8	2013	Framework for secure cloud computing.	Kashif Munir et al	In this paper author review on security challenges in cloud computing and proposed a security model and framework for secure

				<p>the cloud computing environment.</p> <p>That identified the security requirement, attacks, thread, concerns associated to cloud environment of cloud.</p>
9	2009	Cloud Security Issues	B. R. Kandukuri et al	<p>In this paper they focus on the security issues in cloud computing. The Cloud Security Alliance is a nonprofit organization formed to promote the use of best practices for giving security affirmation inside Cloud Computing, and give instruction on the employments of Cloud Computing to help secure every single type of computing. The Open Security Architecture is another organization focusing on security issues.</p>

## 2.2 Related Work

Cloud computing comes with numerous possibilities and challenges simultaneously. Of the challenges, security is considered as a crucial hindrance for cloud computing in its evolution as a technology (A. Kundu et. al., 2010). Cloud clients' very own information security is along these lines, a critical worry in a cloud computing environment (G. Thippa Reddy et. al.). While providing data security for customers' personal or business related data by only applying the simple strategic policies or specifically applying alone technical security is insufficient to deal with all type of security issues to maintain the high quality of service (L. Wang et. al., 2008). Another factor that acts as a detrimental factor in acceptance of usage of cloud organization is integrity or trust (Hyseni et. al., 2019). ). This is because it directly related to the authenticity, Authorization, and accessibility of the cloud pro associations. Establishing trust or integrity may transform into the best approach to develop a compelling cloud based computing system. In context to the cloud, the trust depends on several features like computer assisted management, procedures and approaches (P. Anand, 2016). The Cloud Security Alliance is a nonprofit organization formed to promote the use of best practices for giving security affirmation inside Cloud Computing, and give instruction on the employments of Cloud Computing to help secure every single type of computing. The Open Security Architecture is another organization focusing on security issues [5]. Where the former one deals with the hardware and software utilization, the latter one is restricted to availing various utilities and not the hardware from the cloud service and infrastructure providers [13]. In some specific situations, for instance, information protection is that it exceptionally asked to get detecting secure information progressively, which was practically unthinkable for little size endeavors

that utilized their own frameworks [8].

<b>Table 2.2 Contribution table by Experts with Year</b>			
<b>Experts</b>	<b>Year</b>	<b>Contribution</b>	<b>Methodology</b>
<b>L. Wang et. al.</b>	2008	A study on cloud computing	Theocratically
<b>R. Maggiani et. al.</b>	2009	Cloud computing is discussed with communication	Theocratically
<b>A. Kunduet. al.</b>	2010	Introduced new services	Method based
<b>Akhil Behl et. al</b>	2011	Emerging Security Challenges in Cloud Computing	Evolutions
<b>Gonzalezet. al.</b>	2012	Current security concerns and solutions for cloud computing	Quantitative analysis
<b>V. Inukolluet. al.</b>	2014	A study on security issues associated with Big Data	Theocratically
<b>G. Thippa Reddyet. al.</b>	2015	Framework for Cloud security	Validated
<b>P. Anandet. al.</b>	2016	Threat Assessment	Quantitative Assessment
<b>D. H. Adnaan Arbaaz Ahmedet. al.</b>	2018	Study of Security Issues and Research Challenges	Evaluation
<b>Hyseniet. al.</b>	2019	Proposed a model related to cloud	Quantification

		security	
--	--	----------	--

## 2.3 CONCLUSION

Many authors have been tried to analyze security in cloud computing and also detecting issues and they proposed many techniques for reducing security issues. Different parameters like authentication, authorization, non repudiation of cloud security. In our proposed native approach we used AHP tools for detecting parameter for the best security parameter. The proposed approach in this paper decreases the security issues in the network and improves the efficiency of the network.

## **CHAPTER: 3**

### **PROPOSED WORK AND METHODOLOGY**



## **INTRODUCTION**

Cloud security issues Organization uses various cloud services as IaaS, PaaS, SaaS and the models like public, private, hybrid. These models and services has various cloud security issues. Each service model is associated with some issues. Security issues are considered in two views first in the view of service provider who insures that services provided by them should be secure and also manages the customer's identity management. Other view is customer view that ensures that service that they are using is secure enough [5].

### **Cloud Authorization**

Authorization management in the cloud should ensure that users have appropriate rights to access cloud as well as enterprise managed resources. Both policy definition and enforcement functions need to be available. User access needs to be approved or disapproved in real time with respect to the authorization policies in place [4]. Completely trusted and anonymous authorization should be restricted, and detailed user authorization should be implemented. This needs to work seamlessly across on-premise systems and the enterprise in the cloud, offering real-time synchronization for both provisioning and de-provisioning.

### **Cloud Authentication**

Authentication is the process of verifying the credentials of an entity trying to access a protected resource. Authentication must be done in a secure, trustworthy, and manageable manner [8]. For accounts that require higher levels of security, multiple factor authentications may be required. Authentication systems should have the capability to use business transaction risk definition as guidance, and provide adaptive authentication based on the level of risk of the transaction [12]. Single Sign-On (SSO)

is the functionality within access management where user is authenticated once and the credentials for the session are trusted across different applications within a security domain [7]. This is typically done within one security or risk domain. SSO is a critical requirement within organizations operating all applications within a specific cloud infrastructure.

### **Cloud Non-Repudiation**

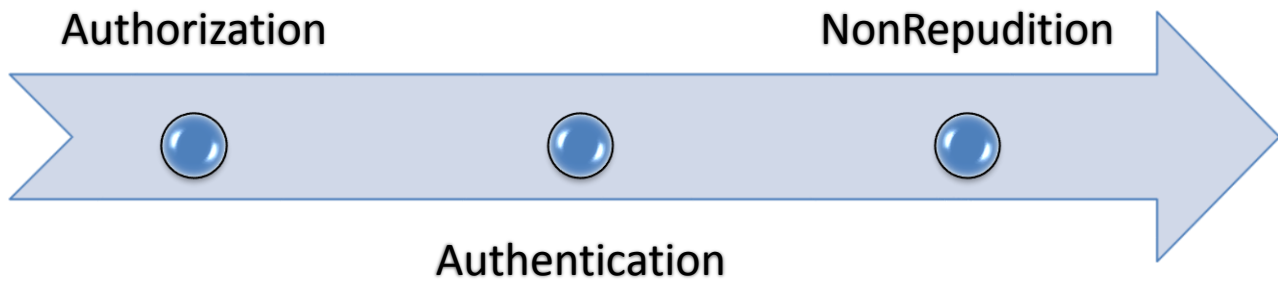
It is always challenging to ensure true non-repudiation, outsourcing IAM to a SaaS provider may make this even more difficult due to the trust boundaries between provider and subscriber. Examples of scenarios that might trigger non-repudiation concerns include:

- Login from multiple systems (Smartphone, desktop/laptop)
- Known Impersonation during trouble-shooting

Access from home desktop/laptop OR internet cafés which do not have a static IP

### **PROPOSED CLOUD SECURITY MODEL DEVELOPMENT**

Cloud Security model has been developed on these three parameters, Authorization, Authentication and Non-Repudiation. This model is a Super Decisions software model. In this model, AHP is used to select a best Security model.



**Figure 3.3 Cloud Security Model**

Figure 1 is used to show the pictorial representation cloud security model on the basis of Authorization, Authentication and Non Repudiation.

**Table 3.1 Preference of Security Criteria**

Criteria	Authorization	Authentication	Non Repudiation
Authorization	1		
Authentication		1	
Non Repudiation			1

Table 1 Show the Preference over the other criteria's. Same set of Criterion shows identity that means no preference over same parameters.

### Empirical Validation Of Proposed Models

Here in the table 2 for each parameter that are Authorization, Authentication, and Non Repudiation are set on different level of cloud security so that we can judge these based on paired comparison and made four combination.

**Table 3.2 Intensity of preference between different criteria**

	7	5	1	5	7	
Authorization	H_secure	L- Secure	Secure	L_secure	H_Secure	Authentication
Authentication	H_secure	L- Secure	Secure	L_secure	H_Secure	Non- Repudiation
Non Repudiation	H_secure	L- Secure	Secure	L_secure	H_Secure	Authorization

**Table 3.3 Intensity Chart**

<b>Intensity of Importance</b>	<b>Definition</b>	<b>Explanation</b>
1	Equal importance	Two activities contribute equally to the objective
3	Moderate importance	Experience and judgment slightly favor one activity over another
5	Strong importance	Experience and judgment strongly favor one activity over another
7	Very strong or demonstrated importance	An activity is favored very strongly over another; its dominance demonstrated in practice
9	Extreme importance	The evidence favoring one activity over another is of the highest possible order of affirmation

**Table 3.3 Full matrix based on paired comparisons**

Criterion	Autharization	Authentication	NonRepudation
Autharization	1	1/5	1/7
Authentication	5	1	1/5
NonRepudation	7	5	1

When we put these scores in the matrix, the diagonal is always 1. We fill in the top triangle of the matrix as shown below on the left matrix. To complete the full matrix, we use the reciprocal values of the upper diagonal. The full, completed matrix is seen on the right side below, Table4.

**Table 3.5a Original Score**

Original Score				
Criterion	Weight	X	Y	Z
Authorization	9%	0.73	0.19	0.08
Authentication	24%	0.08	0.73	0.19
Non-Repudiation	67%	0.06	0.27	0.67
	Total	0.87	1.18	0.94

**Table 3.5b Weighted Score**

	Weighted Score			
	X	Y	Z	
Authorization	0.064	0.017	0.007	0.064
Authentication	0.020	0.177	0.046	0.177
Non-Repudiation	0.042	0.178	0.450	0.450
	0.126	0.371	0.503	

**Table 3.5c Final Weight Score**

Final Weight			
	X	Y	Z
Authorization	1.00	0.26	0.11
Authentication	0.11	1.00	0.26
Non-Repudiation	0.09	0.39	1.00
	1.20	1.65	1.37

These table 3.5a, 3.5b, 3.5c are responsible for calculating the score of respective criteria. If the value of Consistency Ratio is less or equal to 10%, the inconsistency is

acceptable. If the Consistency Ratio is larger than 10%, we need to consider revising our subjective judgments.

**Table 3.4 Authorization Score**

Authorization	M1	M2	M3
M1	1	5	7
M2	0.20	1	3
M3	0.14	0.200	1

Table 6 is responsible for individual score of Authorization criteria, this assures the customer that his/her data is highly Authorization at all phases in cloud.

**Table 3.5 Authentication Score**

Authentication	M1	M2	M3
M1	1	0.200	0.1429
M2	7	1	0.200
M3	7	5	1

Table 7 is responsible for individual score of Authentication criteria, this assures the customer that his/her data is highly Authentication at all phases in cloud.



**Table 3.6 Non-Repudiation Score**

Non-Repudiation	M1	M2	M3
M1	1	5	7
M2	1/5	1	5.00
M3	0.14	0.20	1

Table 8 is responsible for individual score of Non-Repudiation criteria, this assures the customer that his/her data is highly Non-Repudiation at all phases in cloud.

### **I. AHP Methodology**

We will be using method The Analytic Hierarchy Process (AHP), which was a developed by Thomas Saaty that helps in measuring intangible factors that can be relative weights of different parameters by pairing comparisons using judgments from 1 to 9 fundamental scale and resulting according to the priorities of the parameters which are considered in the work. Which is for both tangibles and intangibles and used also in making decision by giving a hierarchical model with a goal, criteria with sub-criteria's and alternatives of making pair for comparison judgments about the dominance of groups of elements in a level below with respect to the element from which they are connected in the level above. In the end the priorities of all the elements are synthesized to rank the alternatives [10]. The hierarchies obtained can be extended

to multi-level decision making models with the hierarchies of interest, right set of circumstances, costs and risks. The AHP has been used in many areas especially in resource allocation and conflict resolution. We must first measure numerous intangibles that have great impact before we can include them as variables. What is most significant is that intangibles can only be measured through expert judgment and only relative to the goals of concern in a situation [11]. The AHP methods are divided in three parts to look at the problem. The first part is to resolve the issue; the second part is the solutions that are available for the problem. The third and the most important part as far as the AHP method is concerned the criteria used to evaluate the alternative solutions.

Here the procedure for doing the step in AHP are:

### **Step 1: Define Alternatives**

The AHP process begins by defining the alternatives solution that are needed solve the problem. These alternatives could be different criteria for the solution.

### **Step 2: Define the Problem and Criteria**

This step makes model for the problem. According to AHP methodology, a set of sub problems is related to one problem. The AHP method we work on breaking the problem into small problems. The criteria to evaluate the solutions emerge when we process the breaking down of the sub problem.

### **Step 3: Establish Priority amongst Criteria Using Pair-wise Comparison**

We establish Priority amongst Criteria in this step The AHP method uses pair-wise comparison to create a matrix. For example by weigh the relative importance of protection from downfall vs. Liquidity of the firm. Then in the next matrix, there

will be a pairwise comparison between liquidity and chance of appreciation and so protection from downfall and in the next matrix I say that protection from downfall is half as important as chance of appreciation, then the following situation emerges:

$$\text{Liquidity} = 2 \text{ (Protection from downfall)}$$

- Protection from downfall =  $\frac{1}{2}$  (Chance of appreciation)
- Therefore, Liquidity must equal chance of appreciation

#### **Step 4: Check Consistency**

In this we inbuilt in software tools that help solve problems in AHP.

#### **Step 5: Get the Relative Weights**

In this step the software tool will run the mathematical calculation based on the data and relative weights to the parameters. Once the equation has the weighted criteria ready, one can work on the alternatives to get the solution as best as possible to matches their needs.

.

## **CHAPTER: 4**

### **RESULT ANALYSIS AND DICUSSION**

## 4.1 INTRODUCTION

**Result metrics used for this works are as follows:**

- Pair-wise Comparison
- Relative Weights

On the basis of all these parameters of cloud security, analyzed the results of our proposed native approach. In our native approach define Alternatives, Define the Problem and Criteria, Establish Priority amongst Criteria Using Pair-wise Comparison, Check Consistency, Get the Relative Weights for different security parameters

### ➤ **CASE 1: Pair-wise Comparison**

We establish Priority amongst Criteria in this step The AHP method uses pair-wise comparison to create a matrix. For example by weigh the relative importance of protection from downfall vs. Liquidity of the firm. Then in the next matrix, there will be a pairwise comparison between liquidity and chance of appreciation and so protection from downfall and in the next matrix I say that protection from downfall is half as important as chance of appreciation, then the following situation emerges:

$$\text{Liquidity} = 2 \text{ (Protection from downfall)}$$

- Protection from downfall =  $\frac{1}{2}$  (Chance of appreciation)
- Therefore, Liquidity must equal chance of appreciation.









$$\sum R1 + R2 \dots + Rn$$

2. Or

$$\sum C1 + C2 \dots + Cn$$

3. Repeat step 1 and 2 until row and column sum become identity.

Final computation will be end after identity of each row and each column sum.

➤ **CASE 2: Relative Weights**

In this step the software tool will run the mathematical calculation based on the data and relative weights to the parameters. Once the equation has the weighted criteria ready, one can work on the alternatives to get the solution as best as possible to matches their needs.

**Table 4.2 Original Score**

Original Score				
Criterion	Weight	X	Y	Z
Authorization	9%	0.73	0.19	0.08
Authentication	24%	0.08	0.73	0.19

Non-Repudiation	67%	0.06	0.27	0.67
	Total	0.87	1.18	0.94

**Table 4.3 Weighted Score**

	Weighted Score			
	X	Y	Z	
Authorization	0.064	0.017	0.007	0.064
Authentication	0.020	0.177	0.046	0.177
Non-Repudiation	0.042	0.178	0.450	0.450
	0.126	0.371	0.503	

**Table 4.4 Final Weight Score**

	Final Weight		
	X	Y	Z
Authorization	1.00	0.26	0.11
Authentication	0.11	1.00	0.26
Non-Repudiation	0.09	0.39	1.00
	1.20	1.65	1.37

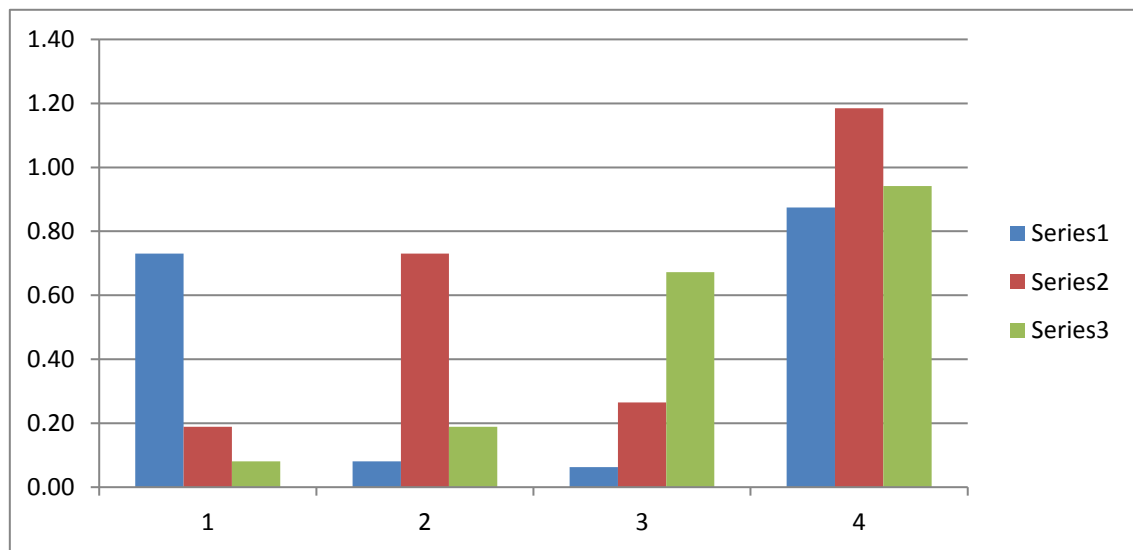
These table 4.2, 4.3, 4.4 are responsible for calculating the score of respective criteria.

If the value of Consistency Ratio is less or equal to 10%, the inconsistency is

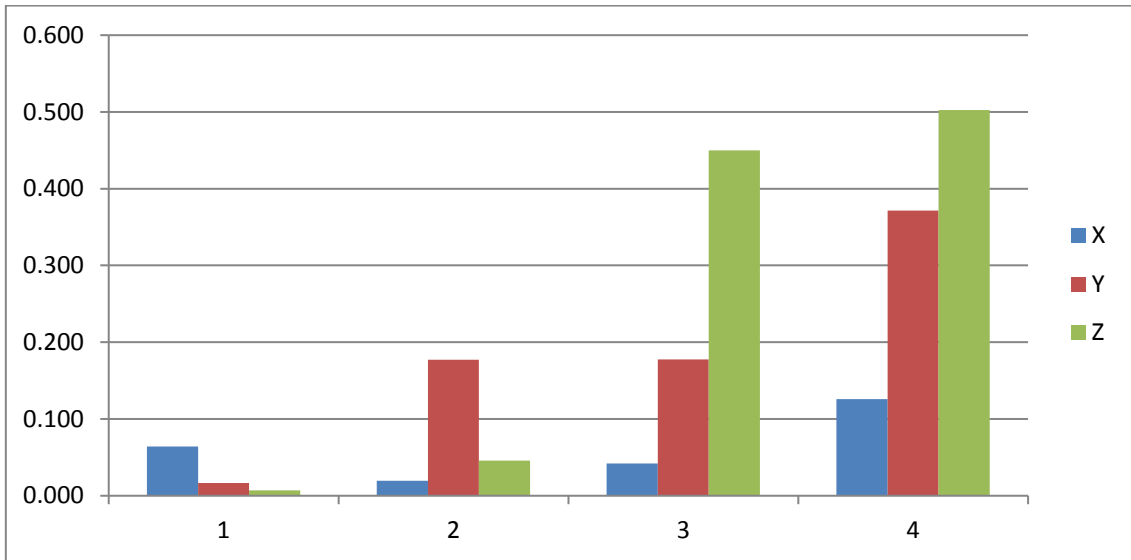
acceptable. If the Consistency Ratio is larger than 10%, we need to consider revising our subjective judgments.

### Comparative analysis of the models

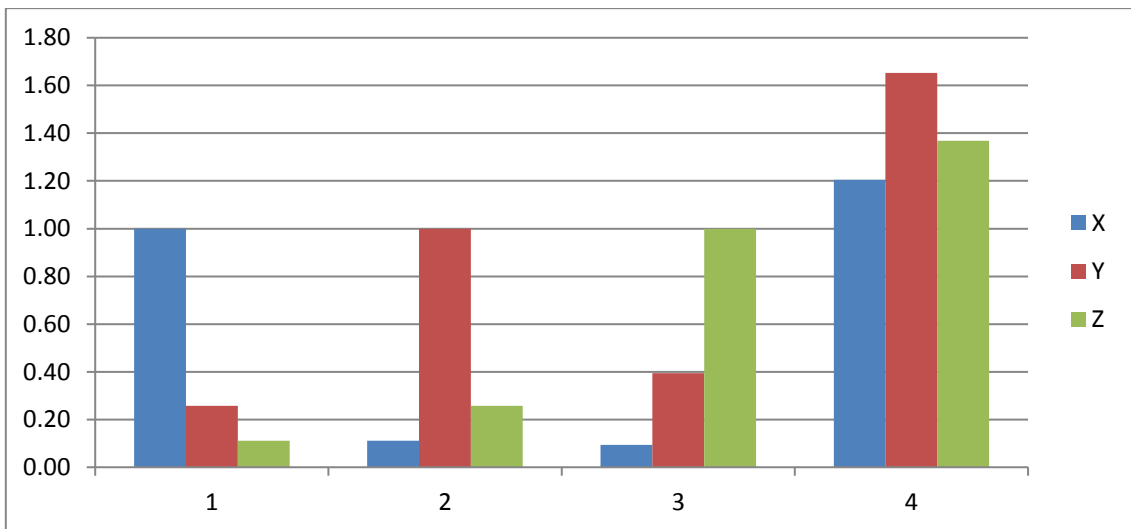
Here in this section we will do the comparative analysis of the given models, for this we will use the weighted score of each criteria that we have calculate with respect to different models and then we will calculate the model with other existing models, for this we will refer to table no 4 in this table weights were calculated.



**Figure 4.1** Comparison of original score



**Figure 4.2 Comparison of Weighted score**



**Figure 4.3 Comparison of Final score**

This figure 2, use to show the comparative graph of original score. And the figure 3, use to show the comparative graph of weighted score. Here x and series 1 stands for authorization, y and series 2 stands for integrity, z and series 3 stands for authentication. Series 4 for final weighted score of respective criteria. Figure 4 has three models of Authorization, Authentication, and Non-Repudiation-based comparison on different models.

## **CHAPTER: 5**

### **CONCLUSION AND FUTURE WORK**

## 5.1 CONCLUSION

Cloud computing is another rising development, which every affiliation these days customize so as to support the adaptability of their relationship in information dissemination, trade. There are few security related issues which could cause nonappearance of security and trust for data and customers assurance, progressive inaction, organizational loss, and sketchy nature of service provider's consistence. The security issue ended up being extra intricate under the cloud model as new expansions have appeared into the troublesome degree identified with the model's data security, customers' assurance mastermind security, along with the stage and establishment issues. This work was performed on basic level study to feature the computational security issues of cloud. The finding of this assessment underlines that there are certain standard issues related with computational execution of cloud which are security factors, cloud environment, data validation and data efficiency. These issues form a basis of research in the field of cloud computing so as to remove the void created by the security issues .This void may be addressed by giving either a particular technique or definite model to reduce these points of concern.

Cloud Security Alliance (CSA) and NIST are the organization which are working on cloud computing security. In this paper we have discussed some security approaches but other approaches are also there that are in the process. Some approaches are also specified which can be used to maintain secure communication and security in a cloud as many systems communicate in it and perform operations. Some approaches are also specified which can be used to maintain secure communication and security in a cloud

as many systems communicate in it and perform operations. Our claim has been proved true. Empirical validation has supported our claim. Finally three different comparisons have been done on the basis of different score.

## **5.2 FUTURE WORK**

In future, we are going to focus on how to maintain more security in cloud computing as day by day users are increasing we need to enhance the security of the data storing in the cloud which is a big data, to make it secure till now no as such security is been given that is 100% data is secured and reliable so in future this field is going to need more focus as there are huge growth opportunities with new technologies coming up. As with new technologies more data will be stored by the users which will need more authorization, authentication and non-repudiation in cloud security which will be a huge challenge for all the stakeholders to maintain.

.

## REFERENCES

- 1) Anjana Tiwari and Inderjeet Kaur “Performance Evaluation of Energy Efficient For MANET Using AODV Routing Protocol ”, 3rd IEEE International Conference on "Computational Intelligence and Communication Technology" (IEEE-CICT 2017) page 1 – page 5
- 2) AbdalftahKaid Said Ali and Dr. U.V. Kulkarni “Comparing and Analyzing Reactive Routing Protocols (AODV, DSR and TORA) in QoS of MANET”, 2017 IEEE 7th International Advance Computing Conference page 345 - page 348.
- 3) HoudaMoudni and Mohamed Er-rouidi “Performance Analysis of AODV Routing Protocol in MANET under the Influence of Routing Attacks”, 2nd International Conference on Electrical and Information Technologies ICEIT’2016 IEEE.
- 4) Vishnu Sharma and AkanshaVij “Security Issues in Mobile Adhoc Network: A Survey Paper ” International Conference on Computing, Communication and Automation (ICCCA2016) IEEE page 561-page 566
- 5) Khan, M. S., Jadoon, Q. K., & Khan, M. I. (2015). A Comparative Performance Analysis of MANET Routing Protocols under Security Attacks. In *Mobile and Wireless Technology 2015* (pp. 137-145). Springer Berlin Heidelberg
- 6) S.V. VASANTHA and DR. A. DAMODARAM “Bulwark AODV against Black hole and Gray hole attacks in MANET ”, 2015 IEEE International Conference on Computational Intelligence and Computing Research.
- 7) NirbhayChaubey “Effect of Pause Time on AODV and TSDRP Routing Protocol



under Black Hole Attack and DOS Attacks in MANET ”,2015 2nd InternationalConference on Computing for SustainableGlobal Development(INDIACom) IEEE page 1807-page 1812

8) Jayson K. Jayabarathan, A. Sivanantharaja “Quality of Service Enhancement in MANET using Priority Aware Mechanism in AOMDV Protocol ”,2015 IEEE UP Section Conference on Electrical Computer and Electronics (UPCON)

9) David Airehrour, Jairo Gutierrez “GradeTrust: A Secure Trust Based Routing Protocol ForMANETs”, 2015 International Telecommunication Networks and Applications Conference (ITNAC) IEEE page 65-page 70.

10) Sandeep Kumar Arora and Mubashir Yaqoob Mantoo “Performance Measurement in MANET ” , 2014 5th InternationalConference- Confluence The Next Generation Information Technology Summit (Confluence) IEEE page 406-page 410

11) Mohammed M. Alani “MANET Security: A Survey ”, 2014 IEEE International Conference on Control System, Computing and Engineering, 28 - 30 November 2014, Penang, Malaysia page 559-page 564.

12) K.Das and A. Taggu “A Comprehensive Analysis of DoS Attacks in Mobile Adhoc Networks ”,2014 InternationalConference on AdvancesinComputing,Communicationsand Informatics (ICACCI)page 2273-page 2278

13) Indira N “Establishing a secure routing in MANET using a Hybrid Intrusion Detection System ”IEEE page 260-page 263

- 14) Anishi Gupta “Black Hole Attack Mitigation Method based on Route Discovery Mechanism in AODV Protocol ”, 2013 IEEE International Conference on Computational Intelligence and Computing Research
- 15) Geethu Mohandas ,Dr Salaja Silas and Shini Sam” Survey on Routing Protocols on Mobile Adhoc Networks ”,©2013 IEEE page 514-page 517.
- 16) Ehsan, H., & Khan, F. A. (2012, June). Malicious AODV: implementation and analysis of routing attacks in MANETs. In Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on (pp. 1181-1187). IEEE.
- 17) Ashok M.Kanthe, Dina Simunic and Ramjee Prasad “Effects of Malicious Attacks in Mobile Ad-hoc Networks” 2012 IEEE International Conference on Computational Intelligence and Computing Research.
- 18) Zaid Ahmad and J.A. Manan” Performance Evaluation on Modified AODV Protocols ”,2012 IEEE Asia-Pacific Conference on Applied Electromagnetics (APACE 2012), December 11 - 13, 2012, Melaka, Malaysia page 158-page 163
- 19) Rutvij H. Jhaveri and S.J.Patel “DoS Attacks in Mobile Ad-hoc Networks: A Survey ”,2012 Second International Conference on Advanced Computing & Communication Technologies IEEE page 535-page 541
- 20) Mehdi Medadian and M.H. Yektaie” Combat with Black Hole Attack in AODV routing protocol in MANET ”,2009 IEEE.
- 21) MarjanKuchaki Rafsanjani “Identifying Monitoring Nodes in MANET by

Detecting Unauthorized and Malicious Nodes ”,2008 IEEE.

22) Frank Kargl, Stefan Schlott, Michael Weber “Identification in Ad hoc Networks ”,Proceedings of the 39th Hawaii International Conference on System Sciences – 2006  
IEEE page 1-page 9

23) N. Meghanathan et al. (Eds.): CCSIT 2011, Part II, CCIS 132, pp. 44–54, 2011.

© Springer-Verlag Berlin Heidelberg 2011

24) Silvia Giordano, Ivan Stojmenovic:  
<https://www.comp.nus.edu.sg/~bleong/geographic/related/giordano04position-routing-survey.pdf>

25) Lei Chen and Chung-wei Lee, IEEE Communications Society / WCNC 2005 0-7803-8966-2/05/\$20.00 © 2005 IEEE form Page 1964 to page 1969

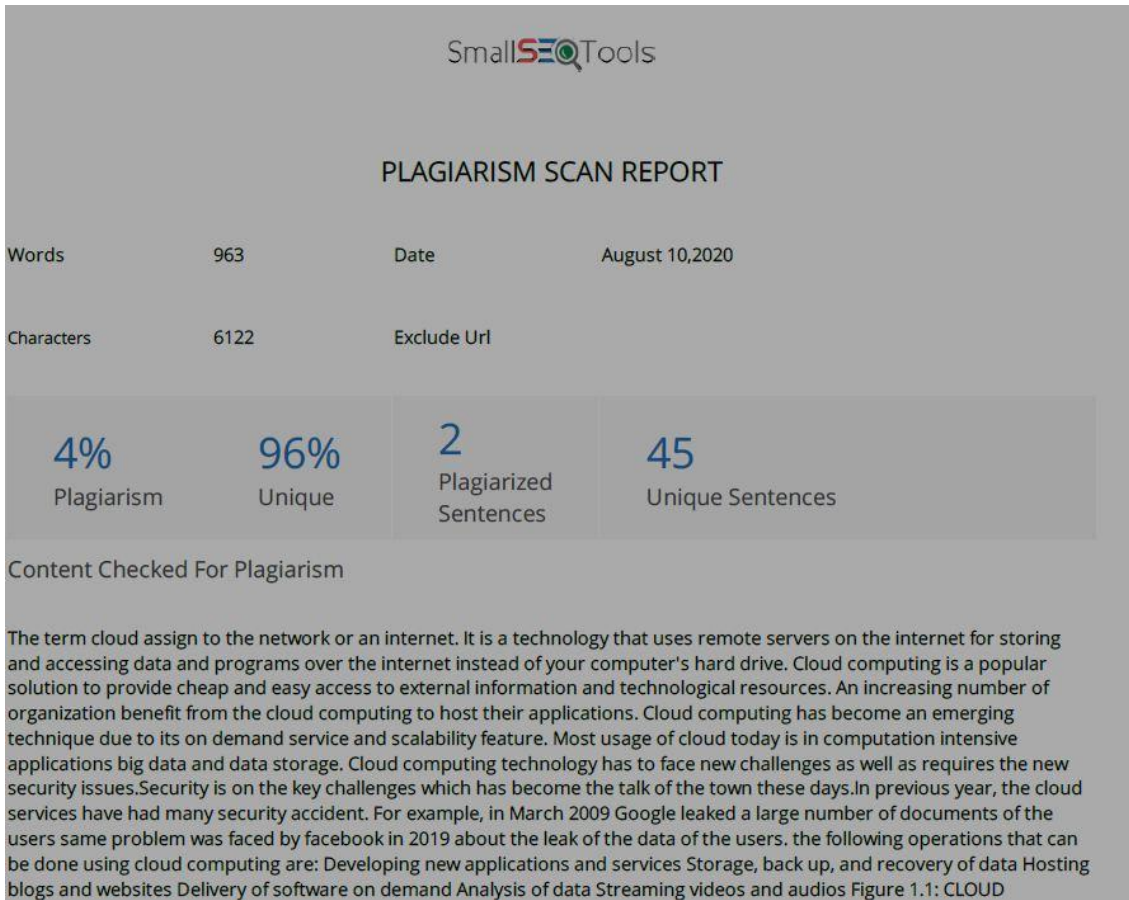
26) Yufei Tao Dimitris Papadias Qiongmao Shen, “Continuous Nearest Neighbor Search ” <https://infolab.usc.edu/csci599/Fall2007/papers/c-5.pdf>

# PLAGIARISM CHECK REPORT

## ABSTRACT



## Introduction



## PLAGIARISM SCAN REPORT

Words 492 Date August 10,2020

Characters 2899 Exclude Url

4%

Plagiarism

96%

Unique

1

Plagiarized  
Sentences

23

Unique Sentences

### Content Checked For Plagiarism

1.4 CHARACTERISTICS OF CLOUD characteristics of Cloud Computing are as follows: Resources are available on large scale, Self-service On-demand, less Maintenance, Network Access at large scale Automatic System Availability, Security Pay for Availability of Resources. Multiple customers are given services which are done with the multi-tenant model. As per the customer's demand many physical and virtual resources are provided for modification. As we know the customer doesn't have the knowledge about where the data is stored and also don't have the control on the data. On-Demand Self-Service is the important features of cloud computing as the user monitors the server uptime continuously with allotted network storage. With this feature, the user monitors the capabilities of the computer. Easy Maintenance the servers are maintained easily and the downtime are very low but some cases have no downtime. The cloud computing gives update for time to time to make it better in performance. The updates are made to make the device more compatible with fixing the bugs and make the performance work faster. Large Network Access The user can update modify aur delete the data from the cloud by just having an internet connection and a device which supports internet connection. These capabilities can be accessed with the internet

### PLAGIARISM SCAN REPORT

Words: 597 Date: August 10,2020

Characters: 3904 Exclude Url



#### Content Checked For Plagiarism

TYPES OF CLOUD COMPUTING according to business needs there are four different cloud models: Private Cloud: It is the cloud which is provided for use of any one particular organisation or company. This method is mostly used for intra-business purpose. Where the cloud deployed in the organisation or company are allowed governed, owned and operated by the same company or organisation. Community Cloud: it is the cloud model which is provided to the community. Public Cloud: This type of cloud is usually for B2C that is business to Consumer communication. Here the cloud is owned, governed and operated by business organization or government. Hybrid Cloud: This type of cloud can be used for both type of communications B2B that is Business to Business or B2C that is Business to Consumer. Figure 1.5 Types of Cloud TYPES OF CLOUD SERVICE MODEL Infrastructure as a service: Infrastructure-as-a-Service provides access to fundamental resources such as physical machines, virtual machines, virtual storage, etc. The IAAS offers many other resources: Virtual machine disk storage Virtual local area network (VLANs) Load balancers IP addresses Software bundles Fig.1.6. Infrastructure as a Service Platform as a Service: Platform-as-a-Service offers the runtime environment for applications. It offers development and deployment tools which are

### PLAGIARISM SCAN REPORT

Words: 251 Date: August 09,2020

Characters: 1663 Exclude Url



#### Content Checked For Plagiarism

Limitations of Cloud Computing Here, are significant limitations using Cloud Computing: Performance When we are working in cloud environment, application is running on the server which simultaneously provides resources to other businesses. Any reedy behavior or DDoS attack on tenant could affect the performance of shared resource. Technical Issues Cloud technology is always susceptible to an dimout and other technical issues. Even, the cloud service provider companies may face this type of problem despite maintaining standards of maintenance. Security Threat in the Cloud Another problem while working with cloud computing services is security risk. Before adopting cloud technology, we should be well aware of the fact that they will be sharing all company's sensitive information to a third-party cloud computing service provider. Hackers may access this information. Downtime Downtime can also be considered while working with cloud computing. That's because cloud provider may face power loss, low connectivity of internet, maintenance service, etc. Internet Connectivity Good



# Literature Review

SmallSETools

### PLAGIARISM SCAN REPORT

Words	994	Date	August 10,2020
Characters	6482	Exclude Url	

**9%**  
Plagiarism

**91%**  
Unique

**4**  
Plagiarized Sentences

**39**  
Unique Sentences

Content Checked For Plagiarism

3.1 LITERATURE REVIEW In 2019, Aakriti Sharma et al published an article Authentication Issues and Techniques in Cloud Computing Security: A Review, in this paper author discuss the methods of user's authentication and challenges faced in cloud computing. And discuss about the security issues in cloud computing and make an observation on user authentication techniques. In 2019, Dhurate Hyseni et al published an article The Proposed Model to Increase Security of Sensitive Data in Cloud Computing in this they proposed a security model in cloud working on different conditions, especially for those environment that work is based on sensitive data and those companies that still hesitates to deploy in cloud. In 2019, V. Carchiolo et al published an article Authentication and Authorization Issues in Mobile Computing: A Case Study in this paper author discuss issues in mobile cloud computing and presented the solution of authorization and authentication issues in mobile cloud computing. By applied within the STMicroelectronics IC manufacture plants. It's also improve by introducing strong mechanism as trustworthiness. In 2019, Bogdan Cosmin Chifor et al published an article Security Oriented Framework for Internet of thing Smart Home application in this paper author present a security framework for smart Home. They proposed a secure cloud which acts as proxy between the IOT devices and third party functional cloud along with a key escrow scheme which enables a smartphone based authorization mechanism. And solution is an extension for the EAP-NOOB security scheme acting as a command authorization. In 2018, Adnaan Arbaaz Ahmed et al published an article Study of Security Issues and Research Challenges in this paper they discuss various models of cloud computing, security issues and research challenges in cloud environment. In this they also discuss about the multi-tenancy which is also a major issue in cloud computing security. In 2017, Huma Farooq published an article A Review on cloud computing Security Using Authentication Techniques In this paper author discuss about the security issues resolve by using authentication techniques such as username and password, MTM, multifactor, PKI, Single sign On and biometric authentication. In 2017, Gururaj Ramchadra et al published an article A Comprehensive Survey on Security in Cloud Computing. In this paper author summarizes a number of review articles on security



## Proposed work and Methodology

SmallSEOTools

### PLAGIARISM SCAN REPORT

Words	1000	Date	August 10,2020
Characters	6272	Exclude Url	

**0%**

Plagiarism

**100%**

Unique

**0**

Plagiarized Sentences

**49**

Unique Sentences

Content Checked For Plagiarism

CHAPTER: 4 METHODOLOGY AND PROPOSED WORK PROPOSED CLOUD SECURITY MODEL DEVELOPMENT Cloud Security model has been developed on these three parameters, Authorization, Authentication and Non-Repudiation. This model is a Super Decisions software model. In this model, AHP is used to select a best Security model. Figure 1 Cloud Security Model Figure 1 is used to show the pictorial representation cloud security model on the basis of Authorization, Authentication and Non Repudiation. Table 1 Preference of Security Criteria Criteria Authorization Authentication Non Repudiation Authorization 1 Authentication 1 Non Repudiation 1 Table 1 Show the Preference over the other criteria's. Same set of Criterion shows identity that means no preference over same parameters. Empirical Validation Of Proposed Models Here in the table 2 for each parameter that are Authorization, Authentication, and Non Repudiation are set on different level of cloud security so that we can judge these based on paired comparison and made four combination. Table 2 Intensity of preference between different criteria 7 5 1 5 7 Authorization H\_secure LSecure Secure L\_secure H\_Secure Authentication Authentication H\_secure L-Secure Secure L\_secure H\_Secure Non-Repudiation Non Repudiation H\_secure L-Secure Secure L\_secure H\_Secure Authorization Table 3 Intensity Chart Intensity of Importance Definition Explanation 1 Equal importance Two activities contribute equally to the objective 3 Moderate importance. Observation and judgment favour one activity over another five Strong important observation and judgment strongly favour one activity over another seven Very strong importance An activity is considered very strongly over another; its superiority demonstrated in practice nine Extreme importance. The method favour one activity over another is of the highest possible order of affirmation. Table 4 Full matrix based on paired comparisons Criterion Authoriazation Authentication NonRepudiation Authoriazation 1 1/5 1/7 Authentication 5 1 1/5 NonRepudiation 7 5 1 1 When we put these scores in the matrix, the diagonal is always 1. We fill in the top triangle of the matrix on the left matrix as shown. To complete the matrix, we use the reciprocal values of the upper diagonal. The full, completed matrix is seen on the right side below, Table4. Table 5a Original Score Original Score Criterion Weight X Y Z Authorization 9% 0.73 0.19 0.08 Authentication 24% 0.08 0.73 0.19 Non-Repudiation 67% 0.06 0.27 0.67 Total 0.87 1.18 0.94 Table 5b Weighted Score Weighted Score X Y Z Authorization 0.064 0.017 0.007 0.064 Authentication 0.020 0.177 0.046 0.177 Non-Repudiation 0.042 0.178 0.450 0.450 0.126 0.371 0.503 Table 5c Final Weight Score Final Weight X Y Z Authorization 1.00

## Result and Analysis

SmallSEOTools

### PLAGIARISM SCAN REPORT

Words	770	Date	August 10,2020
Characters	5313	Exclude Url	

**4%**

Plagiarism

**96%**

Unique

**1**

Plagiarized Sentences

**23**

Unique Sentences

Content Checked For Plagiarism

Performance metrics used for this works are as follows: Pair-wise Comparison Relative Weights On the basis of all these parameters of cloud security, analyzed the results of our proposed native approach. In our native approach define Alternatives, Define the Problem and Criteria, Establish Priority amongst Criteria Using Pair-wise Comparison, Check Consistency, Get the Relative Weights for different security parameters CASE 1: Pair-wise Comparison The AHP method uses pair-wise comparison to create a matrix. For example the firm will be asked to weigh the relative importance of protection from downfall vs. liquidity. Then in the next matrix, there will be a pair-wise comparison between liquidity and chance of appreciation and so protection from downfall and in the next matrix I say that protection from downfall is half as important as chance of appreciation, then the following situation emerges: Liquidity = 2 (Protection from downfall) Protection from downfall = ½ (Chance of appreciation) Therefore, Liquidity must equal chance of appreciation. Table 9 Pair-wise Comparison 1 0.20 0.14 5 1 0.20 7 5 1 13 6.20 1.34 0.07692308 0.03225806 0.10638298 0.21556412 0.35684546 0.14964487 0.49350967 1 0.38461538 0.16129032 0.14893617 0.69484188 0.55352937 0.23212522 0.21434541 1 0.53846154 0.80645161 0.74468085 2.089594 0.25768716 0.38593699 0.35637586 1 1 1 1.16806198 0.76770707 1.06423094 0.30550216 0.19492444 0.46372423 0.96415082 0.31686138 0.20217214 0.48096648 1 0.47388698 0.3023617 0.20140874 0.97765743 0.4847168 0.30927163 0.20601157 1 0.23061006 0.50271206 0.22406702 1 0.5910175 0.2004704 0.47506070 0.21645213 1 0.04005700 0.00651255 1 0.0242010

## Conclusion

SmallSEQTools

**PLAGIARISM SCAN REPORT**

Words	303	Date	August 10,2020
Characters	1994	Exclude Url	

<b>0%</b> Plagiarism	<b>100%</b> Unique	<b>0</b> Plagiarized Sentences	<b>13</b> Unique Sentences
-------------------------	-----------------------	--------------------------------------	-------------------------------

Content Checked For Plagiarism

CHAPTER: 5 CONCLUSION 5.1 CONCLUSION Cloud computing is another rising development, which every affiliation these days customize so as to support the adaptability of their relationship in information dissemination, trade. There are few security related issues which could cause nonappearance of security and trust for data and customers assurance, progressive inaction, organizational loss, and sketchy nature of service provider's consistence. The security issue ended up being extra intricate under the cloud model as new expansions have appeared into the troublesome degree identified with the model's data security, customers' assurance mastermind security, along with the stage and establishment issues. This work was performed on basic level study to feature the computational security issues of cloud. The finding of this assessment underlines that there are certain standard issues related with computational execution of cloud which are security factors, cloud environment, data validation and data efficiency. These issues form a basis of research in the field of cloud computing so as to remove the void created by the security issues .This void may be addressed by giving either a particular technique or definite model to reduce these points of concern. Cloud Security Alliance (CSA) and NIST are the organization which are working on cloud computing security. In this paper we have discussed a some security approaches but other approaches are also there that are in the process. Some approaches are also specified which can be used to maintain secure communication

## PUBLICATION WORK



**Science and Engineering Journal**  
UGC-CARE APPROVED JOURNAL  
ISSN NO: 0103-944X

### ACCEPTANCE LETTER TO AUTHOR

Dear Author,

With reference to your paper submitted "A Cloud Security Model Using AHP" we are pleased to accept the same for publication in **Science and Engineering Journal**, Volume 24, Issue 8, August-2020.

**Manuscript ID: SAE-0820-59**

Please send the scanned copies of Registration form and Copyright form along with Payment Screenshot.

Processing charges for maintaining article online and soft copy of the E-Certificate the registration fee is ₹ 2000. Please note that the amount we are charging is very nominal & only an online maintenance and processing fee.

#### The Processing Fee Includes


Online Publication & E-certificates
Online maintenance and processing charge
No limitation of number of pages
Editorial fee
Taxes

#### Note:

- Paper will be published online within 24 hours after receiving the fee.
- In case of any query please do not hesitate to contact us a editor.saej@gmail.com early reply is appreciated.
- Fee paid for the publication of the paper does not refund under any circumstances.

**Date**  
15-08-2020

Best regards,  
Jose Roberto Camacho  
[saejournal.com](http://saejournal.com)

  
Jose Roberto Camacho  
Editor-in-Chief



Member of  
**Crossref**



## A Systematic Review on Cloud Computing Security Issues

<sup>1</sup>Azra Zia Ansari, Research Scholar, Department of Computer Science & Engineering, Integral University, Lucknow, India,

<sup>2</sup>Mrs. Kavita Agarwal, Associate Professor, Department of Computer Science & Engineering, Integral University, Lucknow, India

### **Abstract**

*Cloud computing is an approach to manage limitations or include restrains progressively without setting resources into new structure , preparing new work force or favoring new programming. As information exchange is a noteworthy activity in the current life, information security ends up being a significant issue. Before separating the security issues, the significance of distributed or cloud based processing is discussed and the analysis of various issues related to cloud based security has also been done. The security issues identified with cloud computing has been investigated here and a local adaptable security solution for the cloud has been proposed. This paper also looks at the cloud security issues in terms of features like ease of adaptability, access, etc. This work is expected to empower scientists and experts to think about various security threats and work on finding out their effective solutions.*

**Keywords:** *Cloud Computing, Security threats, Cloud Architecture*

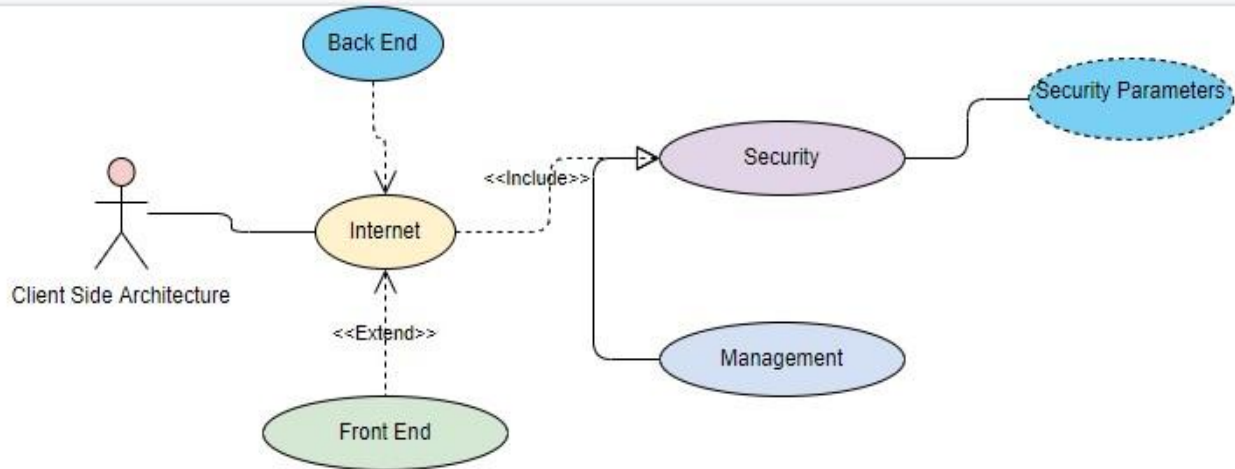
### **I Background**

Since the last decade, cloud computing is seen as an intriguing issue in scholarly zones, attributable to the inherent qualities of the system, by which, we could watch the entire world in an astounding perspective, and specialists of a lot of zones, e. g., worldwide vitality emergency, environmental change, health care,etc [4]benefited from this. Moreover, the improvement of cloud faces the bottleneck, which is brought about by its own exceptionally low security power, low calculation ability and low correspondence capacity. What's more terrible, in some specific situations, for instance, information protection is that it exceptionally asked to get detecting secure information progressively, which was practically unthinkable for little size endeavors that utilized their own frameworks [8].

Consequently, the cloud computing rose as another star in scholastic and business areas. As Cloud processing may get omnipresent in future, various analysts considered the likelihood of joining new subject with distributed computing to take care of the issues which are infer-able from the extraordinary property of issues. Indeed, the blend defeats a few difficulties, for example, stockpiling issues and openness. The on- request benefits trademark that cloud administrations provide, is a significant property to most little estimate undertakings who have constrained asset. In any case, vulnerabilities despite everything exist, particularly in security issues.

For some, it is a perspective that allows ease in handling of resources while for others, it is just a way to deal with programming and accessing the data from the cloud [10]. Cloud computing is well known in association and scholarly nowadays since it gives its clients adaptability and accessibility of information. Moreover cloud computing lessens the cost by enabling the sharing of data to the affiliation. Affiliation can port their data on the cloud with the objective that their financial specialists can use their data. In any case, Cloud gives distinctive office and points of interest yet simultaneously it has a couple of issues related to safe access and limit of data. A couple of issues are there related to cloud security like seller lock-in, multi-tenure, diminished control, interruption of administration, loss of information and so

on. The prime concern is to consider various types of methods to make sure about the cloud model. The cloud computing has expanded wide contemplation, yet there are various security and privacy related issues of appropriated processing have kept the associations from totally enduring cloud stages. The security scenes of dispersed registering occur as frequently as conceivable in some acclaimed associations, for instance, Microsoft, Amazon, Google and other market player. Generally, the security system data is guaranteed by the customers by applying some security strategies, tools and best practices such as including firewall which is similar to the IDS [3]. In any case, the condition is totally extraordinary in distributed computing which is depicted in figure 1. Everything, such as software, hardware, and application data are passed on and taken care of in respective cloud domains. Mosley customer are unaware with the security procedure opted by the companies. Along these lines, there is an uncertainty among customers and cloud suppliers.



**Figure 1 Cloud Computing with security issues**

## II Related Work

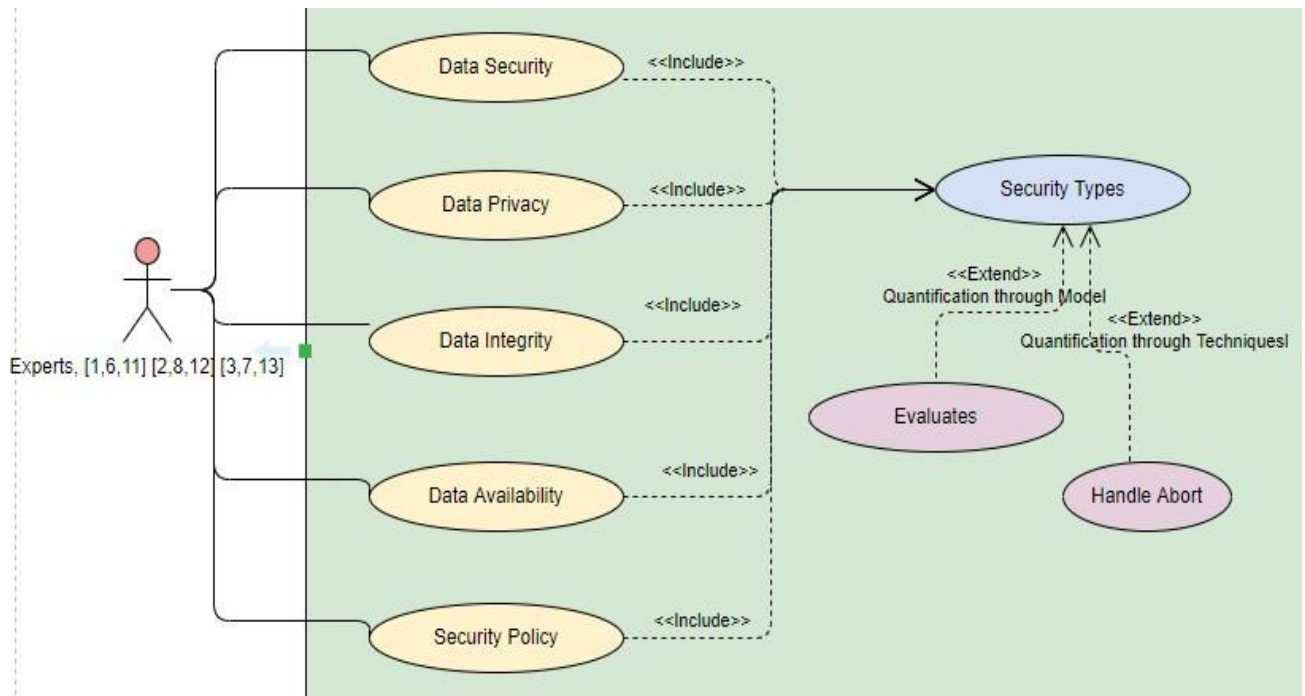
In the span of last few years the concept of cloud has emerged in two broad perspectives – renting of infrastructure on cloud, or renting any utility on cloud. Where the former one deals with the hardware and software utilization, the latter one is restricted to availing various utilities and not the hardware from the cloud service and infrastructure providers [13]. As the cloud based computation evolved with time, the computing world has been presented with various wordings like Software, Platform and Infrastructure as a Service, popularly known as SaaS, PaaS and IaaS. As per previous discussion, the „cloud computing“ is a concept, and so are its terminologies that

define various amalgamations of cloud computing.

Cloud Computing Security issues have been focused by few organizations. The Cloud Security Alliance is a nonprofit organization formed to promote the use of best practices for giving security affirmation inside Cloud Computing, and give instruction on the employments of Cloud Computing to help secure every single type of computing. The Open Security Architecture is another organization focusing on security issues [5]. They have proposed the open security architecture pattern, which is an endeavor to delineate center cloud works, the key jobs for oversight and hazard moderation, collaboration across various internal organizations, and Controls that require additional control. For example,

certification, accreditation and safety assessment series is significantly increased in order to ensure that the operation is being done to another provider "outsourced". Securing the System and Services is pivotal to guarantee that the procurement of administrations is overseen effectively.

Possibility arranging assists with guaranteeing a way of how to react in case of interferences to support conveyance. Figure 2 demonstrates the elevated level perspective on the distributed computing security by the experts.



**Figure 2 Highlighted issues of cloud computing by experts**

Cloud computing comes with numerous possibilities and challenges simultaneously. Of the challenges, security is considered as a crucial hindrance for cloud computing in its evolution as a technology (A. Kundu et. al., 2010). The security challenges for cloud computing have a wide range and they are also evolving on real time basis. Data location is a crucial factor in cloud computing security. Location transparency is one of the conspicuous adaptabilities for cloud computing, which is a security danger

simultaneously – without knowing the particular area of information stockpiling, the arrangement of information insurance represent some district may be seriously influenced and disregarded. Cloud clients' very own information security is along these lines, a critical worry in a cloud computing environment (G. Thippa Reddy et. al.). While providing data security for customers' personal or business related data by only applying the simple strategic policies or specifically applying alone technical security is



insufficient to deal with all type of security issues to maintain the high quality of service (**L. Wang et. al., 2008**). Another factor that acts as a detrimental factor in acceptance of usage of cloud organization is integrity or trust (Hyseni et. al., 2019). This is because it directly related to the authenticity, Authorization, and accessibility of the cloud pro associations. Establishing trust or integrity may transform into the best approach

to develop a compelling cloud based computing system. The course of action of trust model is fundamental in cloud computing because it's an intriguing region for every stakeholder for any given cloud computing scenario. In context to the cloud, the trust depends on several features like computer assisted management, procedures and approaches (**P. Anand, 2016**).

**Table 1 Contribution table by Experts with Year**

<b>Experts</b>	<b>Year</b>	<b>Contribution</b>	<b>Methodology</b>
<b>L. Wang et. al.</b>	2008	A study on cloud computing	Theocratically
<b>R. Maggiani et. al.</b>	2009	Cloud computing is discussed with communication	Theocratically
<b>A. Kunduet. al.</b>	2010	Introduced new services	Method based
<b>Akhil Behl et. al</b>	2011	Emerging Security Challenges in Cloud Computing	Evolutions
<b>Gonzalezet. al.</b>	2012	Current security concerns and solutions for cloud computing	Quantitative analysis
<b>V. Inukolluet. al.</b>	2014	A study on security issues associated with Big Data	Theocratically
<b>G. Thippa Reddyet. al.</b>	2015	Framework for Cloud security	Validated
<b>P. Anandet. al.</b>	2016	Threat Assessment	Quantitative Assessment
<b>D. H. Adnaan Arbaaz Ahmedet. al.</b>	2018	Study of Security Issues and Research Challenges	Evaluation

### III. Critical Observations

After effective study and completion of the precise survey of the available scholarly works, some significant basic perceptions are there which mentioned below in a point wise manner.

- I. Chances are that we upgrade the cloud computing at initial phase of security process which in turn will enormously support the cloud framework and will also be helpful to the customer.
- II. The inclusion of more highlights and functionalities, for example, factors related to security, risk factors and schedule factors in the cloud environment at different phase of security will have positive impact in the pursuit of reducing the risk.
- III. The security factors influencing the cloud framework have to be distinguished and afterward the arrangement of variables, which are important in context to the information security should be concluded.
- IV. Further, initializing and quantifying the security at cloud environment is also important.

### V. Conclusion

Cloud computing is another rising development, which every affiliation these days customize so as to support the adaptability of their relationship in information dissemination, trade. This empowers them to overhaul their benefit, interoperability, limit, and adaptability. Despite numerous advantages in computational environment of the cloud, there are few security

related issues which could cause nonappearance of security and trust for data and customers assurance, progressive inaction, organizational loss , and sketchy nature of service provider's consistence. The security issue has been ended up being extra intricate in various cloud based model as new paradigm have appeared into the most troublesome degree identified with the model's data security and the customers' assurance arrangement. The security issue ended up being extra intricate under the cloud model as new expansions have appeared into the troublesome degree identified with the model's data security, customers' assurance mastermind security, along with the stage and establishment issues. This work was performed on basic level study to feature the computational security issues of cloud. The finding of this assessment underlines that there are certain standard issues related with computational execution of cloud which are security factors, cloud environment, data validation and data efficiency. These issues form a basis of research in the field of cloud computing so as to remove the void created by the security issues . This void may be addressed by giving either a particular technique or definite model to reduce these points of concern.

### Refereces

1. L. Wang, Gregor Laszewski, Marcel Kunze and Jie Tao, "Cloud Computing: A Prespective Study", *New Generation Computing-Advances of Distributed Information*

- Processing*, vol. 28, no. 2, pp. 137-146, 2008.
2. R. Maggiani, "Communication Consultant Solari communication Cloud computing is changing How we communicate", *IEEE International Professional Conference IPCC*, pp. 1-4, July 2009, ISBN 1-42444357-4.
  3. B. R. Kandukuri, R. V. Paturi and A. Rakshit, "Cloud Security Issues," 2009 IEEE International Conference on Services Computing, Bangalore, India, September 21-25, 2009. In Proceedings of IEEE SCC'2009. pp. 517-520, 2009. ISBN: 978-0-7695-3811-2
  4. Ronald L. Krutz, Russell Dean Vines "Cloud Security A Comprehensive Guide to Secure Cloud Computing", Wiley Publishing, Inc.,2010.
  5. Xuan Zhang, Nattapong Wuwong, Hao Li, etc. Information security risk management framework for the cloud computing environments. In Proc. Of 10th international conference on computer and informaiton technology, 2010.
  6. Special Publication 800-30. Guide for Conducting Risk Assessments. America: National Institute of Standards and Technology, 2011.
  7. European Network and Information Security Agency (ENISA). Cloud Computing: Benefits, risks and recommendations for information security.2009.
  8. Akhil Behl Emerging Security Challenges in Cloud Computing (An insight to Cloud security challenges and their mitigation) , 2011.
  9. Gonzalez, N., Miers, C., Redigolo, F., Semplicio, M., Carvalho, T., Naslund, M. and Pourzandi, M.. A quantitative analysis of current security concerns and solutions for cloud computing. *Journal of Cloud Computing*, 1(11), 1-18, (2012).
  10. Hamlen, K., Kantarcioglu, M., Khan, L. and Thuraisingham, V. (2010). Security Issues for Cloud Computing. *International Journal of Information Security and Privacy*, 4(2), 39-51. doi: 10.4018/jisp.2010040103.
  11. Youssef, A.E. (2012). Exploring Cloud Computing Services and Applications. *Journal of Emerging Trends in Computing and Information Sciences*, 3(6), 838-847.
  12. Zisis, D and Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, 28, 583-592. doi:10.1016/j.future.2010.12.006.
  13. D. H. Adnaan Arbaaz Ahmed, "Cloud Computing: Study of Security Issues

- And Research Challenges", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), April 2018.
14. D. A. L. B. S. a. B. C. Hyseni, "The Proposed Model to Increase Security of Sensitive Data in Cloud Computing", *International Journal of Advanced Computer Science And Applications*, vol. 9, no. 2, pp. 203-210, 2019.
  15. G. Thippa Reddy, K. Sudheer, K. Rajesh and K. Lakshmana, "Employing Data Mining on Highly Secured Private Clouds for Implementing a Security – as a-Service Framework", *Journal of Theoretical and Applied Information Technology*, vol. 59, no. 2, 2015.
  16. V. Inukollu, S. Arsi, and S. Ravuri, "Security Issues Associated with Big Data in Cloud Computing," *Int. J. Netw. Secur. Its Appl.*, vol. 6, no. 3, pp. 45–56, 2014.
  17. P. Anand, J. Ryoo, H. Kim, and E. Kim, "Threat Assessment in the Cloud Environment – A Quantitative Approach for Security Pattern Selection," in *IMCOM '16*, 2016, p. 8.
  18. A. Kundu, C. D. Banerjee, P. Saha, "Introducing New Services in Cloud Computing Environment", *International Journal of Digital Content Technology and its Applications*, AICIT, Vol. 4, No. 5, pp. 143-152, 2010.
  19. Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, "On technical Security Issues in Cloud Computing," *Proc. of IEEE International Conference on Cloud Computing (CLOUD-II)*, 2009, pp. 109-116, India, 2009