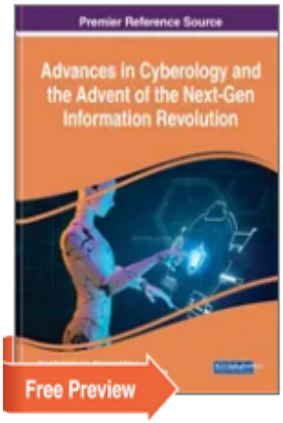
BOOK CHAPTER



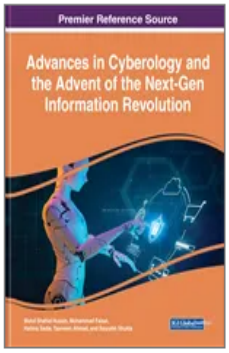
Advances in Cyberology and the Advent of the Next-Gen Information Revolution

Mohd Shahid Husain, Mohammad Faisal, Halima Sadia, Tasneem Ahmad, Saurabh Shukla

Release Date: June, 2023 | Copyright: © 2023 | Pages: 271
DOI: 10.4018/978-1-6684-8133-2
ISBN13: 9781668481332 | ISBN10: 1668481332 | EISBN13: 9781668481356

Table of Contents

CHAPTER 1



Cloud Computing Cyber Threats and Vulnerabilities

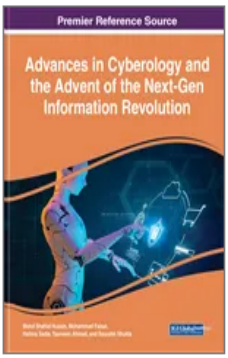
Sami Ouali

Source Title: Advances in Cyberology and the Advent of the Next-Gen Information Revolution
Copyright: © 2023 | Pages: 21
DOI: 10.4018/978-1-6684-8133-2.ch001

Abstract

Cloud computing has become an integral part of modern business operations, with organizations of all sizes and in all industries turning to the cloud to improve efficiency, reduce costs, and increase flexibility. However, the adoption of cloud computing has also introduced a range of new security challenges, as sensitive data and critical systems are moved to cloud-based infrastructure that may be managed by third parties. This chapter discusses the various types of cyber threats that can occur in the cloud, including data breaches, malware, and cloud-based attacks, as well as the measures that organizations can take to protect themselves against these threats on their data, infrastructure, and applications. This chapter examines also the role of cloud providers in securing data in the cloud, and the importance of implementing strong security measures to protect against these threats. By understanding the nature of these threats and the steps that can be taken to mitigate them, organizations and individuals can more effectively protect themselves and their sensitive data in the cloud.

CHAPTER 2



The Critical Analysis of E-Commerce Web Application Vulnerabilities

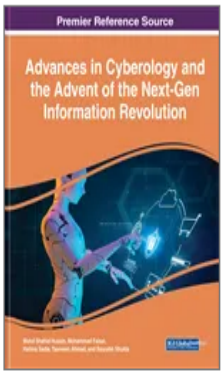
Gausiya Yasmeen, Syed Adnan Afaq

Source Title: Advances in Cyberology and the Advent of the Next-Gen Information Revolution
Copyright: © 2023 | Pages: 16
DOI: 10.4018/978-1-6684-8133-2.ch002

Abstract

Large-scale deployments of web applications occur continuously. The failure to validate or sanitize form inputs, improperly configured web servers, and application design flaws are the main causes of security vulnerabilities that continue to infect web applications, allowing hackers to access sensitive data and using legitimate websites as a breeding ground for malware. These vulnerabilities can be used to compromise the security of the application. The largest problem that enterprises face is how to create a web application that satisfies their needs for safe processes, E-Commerce, and the transmission of sensitive data. OWASP updates and releases a list of the top 10 web application vulnerabilities every few years. Along with the OWASP Top 10 Threats, this chapter also discusses each vulnerability's possible effects and how to avoid them. According to the OWSP (Open Online Application Security Project) Top Ten, this document analyses the most serious web vulnerabilities, their causes, and their impacts.

CHAPTER 3



The Link Between Privacy and Disclosure Behavior in Social Networks

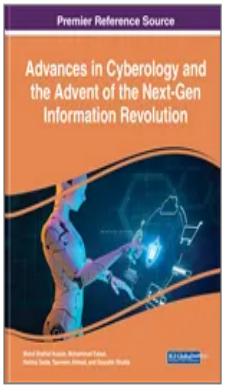
Mohammad Daradkeh

Source Title: Advances in Cyberology and the Advent of the Next-Gen Information Revolution
Copyright: © 2023 | Pages: 24
DOI: 10.4018/978-1-6684-8133-2.ch003

Abstract

Based on the antecedent-privacy concern-outcome (APCO) model of privacy concerns, this study developed a moderated mediation model to investigate the mechanisms by which social media privacy policies (including both privacy policy understanding and perceived effectiveness dimensions) influence self-disclosure. The model was tested in this study using a deductive approach and a quantitative research strategy. In this study, a self-reported questionnaire was used to collect information from social media users. To test the research model and hypotheses, we used multiple regression analysis. According to the results of this study, trust in social media mediated the relationship between privacy policy and self-disclosure, while privacy costs moderated the relationship between privacy policy and trust in social media. Furthermore, the link between privacy policy and self-disclosure is a complex multicollinear model with mediating effects rather than a simple linear model.

CHAPTER 4



Cyber Threat Migration: Perpetuating in the Healthcare Sector and Agriculture and Food Industries

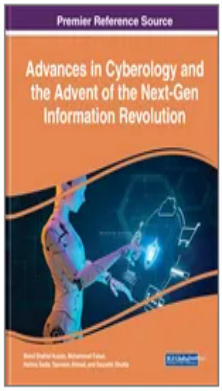
Minhaj Akhtar Usmani, Kainat Akhtar Usmani, Adil Kaleem, Mohammad Samiuddin

Source Title: Advances in Cyberology and the Advent of the Next-Gen Information Revolution
Copyright: © 2023 | Pages: 24
DOI: 10.4018/978-1-6684-8133-2.ch004

Abstract

'Globalization,' 'industrialization,' 'cyber connectivity,' 'digitalization,' and 'e-commerce' are not fantasy words in today's era. They all amalgamated towards the growth and development of every sector in the country. But as on other side of the coin, cyber security is on the verge of serious threats in digital world. The danger posed by cyber security threats in today's world cannot be understated. The health sector, agriculture, and food and beverage industries are no exemptions. As they all are inter-related, they manage an array of assets, including infrastructure, applications, managed and unmanaged endpoints, mobile devices, and cloud services, all of which can be attacked. Information and cyber security are trending topics. As the security risk is scooping high, different organizations should take steps forward to protect themselves. This chapter focuses on the frightening hikes in incidences of cyber-attacks, and also focuses on major cyber security approaches to minimize the risk of cyber breaches and making these industries flourish like never before.

CHAPTER 5



The Critical Impact of Cyber Threats on Digital Economy

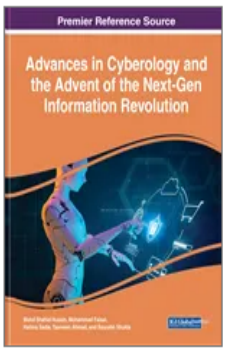
Syed Adnan Afaq, Saman Uzma, Gausiya Yasmeen

Source Title: Advances in Cyberology and the Advent of the Next-Gen Information Revolution
Copyright: © 2023 | Pages: 23
DOI: 10.4018/978-1-6684-8133-2.ch005

Abstract

Internet users need to know that there are many different kinds of threats in the online world. Improving cyber security and keeping private information safe is important for a country's safety and economy. For a country's safety and economy, it's important to improve cyber security and keep private information safe. The term "digital economy" refers to a business for digitally delivered goods and services that are created using electronic business models and linked to a global system of economic and social networks. Cyber risk is the most complex issue of the twenty-first century, arising from a wide diversity of causes such as a hacker, terrorists, criminals, insider groups, foreign states, etc. This study includes cyber threats in the digital world. It emphasizes challenges in the healthcare sector, agriculture and food industries.

CHAPTER 6



Cyber Threats in Agriculture and the Food Industry: An Indian Perspective

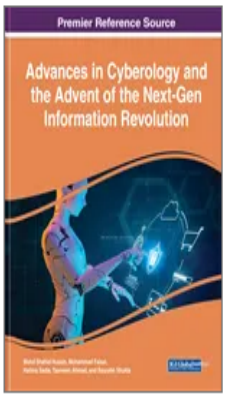
Harish Chandra Verma, Saurabh Srivastava, Tasneem Ahmed, Nayyar Ali Usmani

Source Title: Advances in Cyberology and the Advent of the Next-Gen Information Revolution
Copyright: © 2023 | Pages: 14
DOI: 10.4018/978-1-6684-8133-2.ch006

Abstract

A cyber threat is a harmful act meant to steal, corrupt, or undermine an organization's digital stability. At present cyber threats in agriculture and food industry is a rising concern because farming is becoming more dependent on computers and Internet access. The attacks that fall under this category include denial of service attacks, computer viruses. Growing food demand and shortage of skilled labours have necessitated for the adoption of digital agriculture. The major challenge is to prevent it from cyber threats for successful implementation. As ransomware hackers are increasingly likely to target food supply chain, the food industry is experiencing an increase in cyber-security threats, which might result in business interruptions. Due to the fragile nature of the food supply, the entire food sector needs to be protected . In this chapter, major issue on cyber threats, challenges of cyber-security, some notable cyber-attacks, and cyber-security solutions for the food/agriculture industry are discussed in detail.

CHAPTER 7



Security Issues in the Internet of Things for the Development of Smart Cities

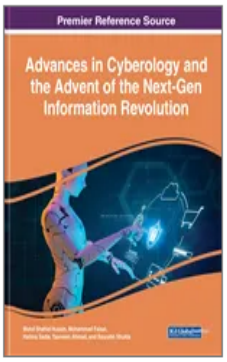
Mohammad Haroon, Dinesh Kumar Misra, Mohammad Husain, Manish Madhav Tripathi, Afsaruddin Khan

Source Title: Advances in Cyberology and the Advent of the Next-Gen Information Revolution
Copyright: © 2023 | Pages: 15
DOI: 10.4018/978-1-6684-8133-2.ch007

Abstract

A city is defined as a group of living and nonliving objects; cities generally have good systems for housing, transportation, hygiene, services, among other things. In prior years, a larger amount of the population was rural, whereas in modern times, the concept of urbanization and a mass exodus to cities has had a profound impact of sustainability on a global scale. A smart city is a concept that participates in information and communication technology with the use of various physical devices to help reduce and optimize the city's daily routine. When thinking of a smart city, one can imagine a layered architecture with infrastructure at the bottom; and connectivity accessibility in security systems in the middle; and at the top are different services that are gearted towards various consumers of the city.

CHAPTER 8



Forensics Analysis of NTFS File Systems

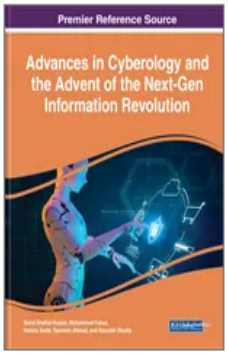
Kumarbhai Shamjibhai Sondarva, Adarsh Kumar, Bhavesh N. Gohil, Sankita J. Patel, Sarang Rajvansh, Ramya T. Shah

Source Title: Advances in Cyberology and the Advent of the Next-Gen Information Revolution
Copyright: © 2023 | Pages: 28
DOI: 10.4018/978-1-6684-8133-2.ch008

Abstract

The internet and computers are reaching everywhere, and all are getting connected through it. Users are utilizing computers to make life easier and work faster. At the same time, many attacks and instances of cybercrime have happened. Therefore, digital forensics is necessary and plays a crucial role. NTFS is one of the most popular file systems used by the Windows operating system, and this chapter provides information for forensic analysis of NTFS file system. This chapter describes digital forensics, stages of digital forensics, and types of digital forensics. NTFS is discussed in brief along with the master file table (MFT). In the same section, it also discusses the method to detect the hidden data in the boot sector, analysis of registry, prefetch, shellbags, and web browsers. They have discussed the collection of volatile and non-volatile data. It also provides the artifacts which an investigator must be seeking, along with the tools used to collect and analyze them and strategies used for investigation and analysis. Data recovery and file carving are also discussed.

CHAPTER 9



Workplace Cyberbullying in the Remote-Work Era: A New Dimension of Cyberology

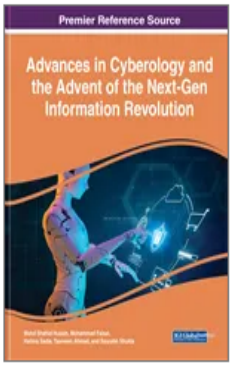
Nashra Javed, Tasneem Ahmed, Mohammad Faisal, Halima Sadia, Emilly Zoë Jeanne Sidaine-Daumiller

Source Title: Advances in Cyberology and the Advent of the Next-Gen Information Revolution
Copyright: © 2023 | Pages: 12
DOI: 10.4018/978-1-6684-8133-2.ch009

Abstract

Information and communication technologies are being used as weapons in a combat zone created by the norm that forces individuals to work from home during this pandemic. The upsurge in workplace cyberbullying is visible in various reports. Workplace cyberbullying may appear to be a less severe form of harassment, but the shift to a more dispersed workforce has made it worse. It is the intimidation experienced by a remote or hybrid employee which results in a breakdown in communication with or mistreatment from leaders. While it makes sense to believe that because we are not at the office, occurrences of antagonism and harassment are drastically reduced, that's not the reality. Spiteful employers and demeaning coworkers might pose a virtual threat. Remote work settings are becoming toxic due to harmful, unkind workplace behavior, including derogatory language, social exclusion, and threats via phone, email, or social media. This chapter unveils a new dimension of cyberology.

CHAPTER 10



The Rise of Deepfake Technology: Issues, Challenges, and Countermeasures

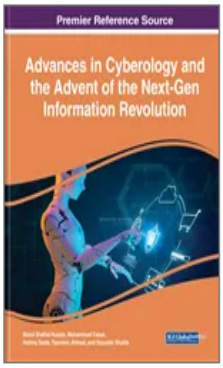
Mohd Akbar, Mohd Suaib, Mohd Shahid Hussain

Source Title: Advances in Cyberology and the Advent of the Next-Gen Information Revolution
Copyright: © 2023 | Pages: 24
DOI: 10.4018/978-1-6684-8133-2.ch010

Abstract

Deepfake technology is an emerging technology prevailing in today's digital world. It is used to create fake videos by exploiting some of the artificial intelligence (AI) based techniques and deep learning methodology. The facial expressions and motion effects are primarily used to train and manipulate the seed frame of someone to generate the desired morphed video frames that mimic as if they are real. Deepfake technology is used to make a highly realistic fake video that can be widely used to spread the wrong information or fake news by regarding any celebrity or political leader which is not created by them. Due to the high impact of social media, these fake videos can reach millions of views within an hour and create a negative impact on our society. This chapter includes the crucial points on methodology, approach, and counter applications pertinent to deep-fake technology highlighting the issues, challenges, and counter measures to be adopted. Through observations and analysis, the chapter will conclude with profound findings and establishes the future directions of this technology.

CHAPTER 11



An Extensive Study and Review on Dark Web Threats and Detection Techniques

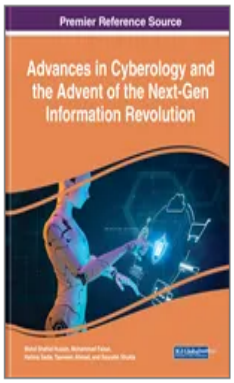
Wasim Khan, Mohammad Ishrat, Mohd Haleem, Ahmad Neyaz Khan, Mohammad Kamrul Hasan, Nafees Akhter Farooqui

Source Title: Advances in Cyberology and the Advent of the Next-Gen Information Revolution
Copyright: © 2023 | Pages: 18
DOI: 10.4018/978-1-6684-8133-2.ch011

Abstract

The Dark Web is a difficult and anonymous network used by cybercriminals, terrorists, and state-sponsored agents to carry out their illicit goals. Dark web cybercrime is very similar to offline crime. However, the vastness of the Dark Web, its unpredictable ecology, and the anonymity it provides are all obstacles that must be overcome in order to track down criminals. To reach the dark web, which is not indexed by search engines, you must use the anonymous Tor browser. The anonymity and covert nature of the network make it ideal for criminal activity and the launch of carefully orchestrated, malicious assaults. Online criminal activity is rampant and getting more intense, according to specialists in cyber security. This chapter has provided a thorough analysis of the various attacks and attack strategies utilized on the dark web. In addition, the authors examine the strengths and weaknesses of the various methods currently in use for threat detection, and how they apply to anonymity networks such as Tor, I2P, and Freenet.

CHAPTER 12



Recent Advances in Cyber Security Laws and Practices in India: Implementation and Awareness

Neyha Malik, Firoz Husain, Anis Ali, Yasir Arafat Elahi

Source Title: Advances in Cyberology and the Advent of the Next-Gen Information Revolution
Copyright: © 2023 | Pages: 22
DOI: 10.4018/978-1-6684-8133-2.ch012

Abstract

The growth of the internet and proliferation of applications, products, and services has given rise to cyber threats which require far more stringent security measures than ever before. Some common types of cybercrimes are job fraud, phishing, baiting, vishing, smishing, credit and debit card fraud, child pornography, cyberbullying, etc. Cyber laws need constant upgrading and refinement to keep pace with the increasing technology. In India, various statutes and initiatives have been launched to ensure its cyber security such as Information Technology Act, 2000 (IT Act), Indian Penal Code, 1860 (IPC), National Cybersecurity Framework (NCFS), financial assistance, Cyber Crime Prevention against Women & Children (CCPWC), Indian Cyber Crime Coordination Centre (I4C), National Cyber Crime Reporting Portal, Citizen Financial Cyber Fraud Reporting and Management System, Indian Computer Emergency Response Team (CERT-In), and Ministry of Electronics & Information Technology (MeitY).