Proceedings of the 3rd International Conference on Signal Processing and Machine Learning
DOI: 10.54254/2755-2721/4/2023326

Computer network information security and protection strategies in the era of big data

Yuxuan Sun

Heriot-Watt University, Edinburgh, U.K., EH14 4AS

albertexert@gmail.com

Abstract. The Internet has entered the big data era, and as more and more businesses employ big data, cloud computing, the Internet of Things, artificial intelligence, and other technologies, the amount of data on the Internet as a whole has also grown dramatically. While Big Data technology has improved the efficiency of many companies, it has also brought challenges for computer network information security protection technology, including massive data privacy leaks that seriously jeopardize the privacy of Internet users. This paper synthesizes literature review findings proving that computer network information security in the big data era has the characteristics of universality, suddenness, concealment, and intelligence in order to address this issue. It also studies the main network information security technologies, such as network situational awareness, vulnerability scanning, intrusion detection and firewall, and identity authentication. In addition, the paper finds that the current problems of network information security mainly include phishing attacks, computer viruses, ransomware, denial of service attacks, APT attacks and threats from inside the network. Finally, the paper explores a number of protective measures to address existing security issues, including the development of network monitoring and threat intelligence systems, the implementation of access control and authentication technologies, network isolation methods, regular software scanning and updates, and organising internal staff security training. Through this study we are able to fully understand the overall pulse of current computer network information security technology and development trends in the era of Big Data, thus providing a more comprehensive and accurate reference for Big Data-related participants to develop responsive information security protection measures and strategies to provide designation.

Keywords: Big Data, Computer Networks, Information Security, Security Protection.

1. Introduction

Massive, heterogeneous, and complicated data have been produced as a result of the quick development and widespread use of several emerging technologies, including the Internet of Things, cloud computing, 5G, and big data technologies. Numerous industries, including finance, healthcare, politics, and transportation, can take advantage of the enormous processing opportunities this data offers. Massive amounts of complicated data can be collected, analyzed, and visualized to aid relevant departments in decision-making and to boost cloud-based productivity. Big Data presents a number of difficulties because it is a popular target for security threats. The Big Data era has created a more difficult information security environment for computer networks as a result of the exponential development in

DOI: 10.54254/2755-2721/4/2023326

the amount of data travelling across networks and the expanding network coverage. In the age of big data, the loss of personal network information as well as the theft and trafficking of computer network information have seriously impacted social security [1]. In light of this, it is crucial and crucial to strengthen and defend computer network information protection in the era of big data.

This study primarily investigates the variables impacting computer network information security in the big data era through relevant literature research and analysis, current protection technologies, and concerns with computer network information security. The trend of the protection approach for computer network information security in the big data era is then shown. In order to better protect Big Data assets, this paper aims to provide a deeper understanding of the characteristics of computer network information security in the Big Data era. This will enable Big Data-related participants, such as Big Data service providers and platform users, to specify corresponding protective measures in conjunction with their own characteristics.

2. Characteristics of computer network information security risks in the era of big data

2.1. Universality

In the age of Big Data, one of the biggest traits of information security vulnerabilities on computer networks is their pervasiveness. Data collected from various terminals, data from application systems, data from external units, data from Internet crawlers, etc. are only a few examples of the various sorts of big data. Given that the sources of information security threats in the Big Data era may include mobile devices, servers, email files, cloud applications, etc. in a range of applications [2], it is evident that the attack surface is very large.

2.2. Sudden

Because the risk is present across the entire attack surface and the current threat perception technology can only be predicted based on past historical experience, some damage, destruction, or failure by unpredictable errors and attacks are difficult to predict and have suddenness. This is especially true for computer network information security risk in the big data era [3].

2.3. Hiddenness

The high degree of concealment, which is brought on by the features of the threat itself, is another feature of computer network information security hazards in the age of big data [4]. For example, APT (Advanced Persistent Threat Attack) and so on are after a long time lurking again among big data platforms and users to carry out vulnerability infiltration so as to steal user data and so on, this kind of behavior usually after a long time maintenance and planning, and has a high degree of concealment [5]. In addition, viruses and Trojan horses can lurk in the computers of ordinary users for a long time by means of hidden channels, and the consequences can be very serious if timely protection measures are not taken.

2.4. Intelligence

A variety of artificial intelligence-based information security threat tactics have evolved as a result of the advancement of artificial intelligence technologies. For example, Deepfake [6], a face recognition technology, is used to falsify the appearance of another person to authenticate the user in order to steal important assets. In a driverless scenario, for example, an attacker could falsify camera data to attack an unmanned car and cause it to misjudge and crash [7]. Such information security threats are constantly being raised and validated in today's rapidly evolving technological environment. As a result, in the big data era, information security dangers in computer networks are dynamic and continually moving towards intelligence.

DOI: 10.54254/2755-2721/4/2023326

3. Common computer network security techniques in the era of big data

In order to defend computer networks against attackers and secure critical infrastructure and data in the era of Big Data, it is essential that you as the maintainer and manager of a network facility use the right tools, techniques and procedures to protect yourself. This paper summarises, through literature research, the following common security techniques currently used in computer networks:

3.1. Network situational awareness techniques

First we must understand where we are vulnerable to attack; this is where cyber situational awareness comes into play. Cyber situational awareness entails leveraging technologies such as cyber security tools to enable organisations to collect, analyse and respond to threat data, understand current risks and predict future risks and design or identify solutions needed to strengthen cyber security posture and improve risk management plans

3.2. Vulnerability Scanning Techniques

Vulnerability scanning technology focuses on examining potential exploit points on a computer or network to identify security vulnerabilities, and this technique is commonly used in the Big Data era as an effective means of analysing hidden vulnerabilities that exist in one's Big Data platform [8]. Computers, Big Data information networks, and communication devices all have system vulnerabilities that vulnerability scan detection finds, analyzes, and predicts the efficacy of remedies, producing extensive analysis reports. In order to find security vulnerabilities, vulnerability scanning programs like NMAP first look for potential attack points, then compare the target attack surface's specifics to a database of data about known security flaws in services and ports, packet construction anomalies, and potential paths to exploitable scripts or programs, and then generate the corresponding analysis reports [9].

3.3. Intrusion detection and firewall technology

Two of the most popular and important tools for protecting data in computer networks are firewalls and intrusion detection systems. While intrusion detection technology (IDS) is the process of monitoring and identifying unwanted attempts to access or modify systems, a firewall's main function is to restrict network traffic in order to prevent unauthorized access to computer networks. We can imagine a firewall as a security guard at the door and an IDS device as a security camera behind the gate. To effectively identify intruding attackers and protect their environment by implementing the necessary protective measures, a combination of the two is typically required in the age of big data [10].

3.4. Authentication technology

Authentication technology, which restricts access to systems by confirming that a user's credentials match those held in an authorized user database or data authentication server, is the most widely used technology in computer networks during the Big Data era [11]. System security, process security, and enterprise information security are all ensured via authentication. For instance, while login into a big data platform, a user must submit a user name and password. In some cases, it is also necessary to input a mobile phone authentication number. Cryptographic authentication techniques, biometric identification techniques like facial recognition, and a combination of these technologies are frequently used for authentication.

4. Problems of computer network information security in the era of big data

Information security is more vital than ever due to the growing threats to network security in the big data era. Therefore, all important parties must be aware of the present difficulties and threats to network information security in the context of big data. The Big Data era's usual information security problems with computer networks include the following.

DOI: 10.54254/2755-2721/4/2023326

4.1. Phishing Attacks

Phishing attacks take the form of instant phishing emails or messages that are created to look legitimate and are intended to deceive individuals into clicking on suspicious links or downloading dangerous software. Phishing operations are one of the most widely used attack vectors nowadays, according to Microsoft statistics [12].

4.2. Computer viruses

Computer viruses are one of the largest security concerns for user data in the modern era. Computer viruses are regularly downloaded from specific websites or sent as email attachments with the goal of harming the user's computer as well as the machines of the user's contacts through systems on the network, such as data theft and destruction.

4.3. Ransomware

Using malicious software or phishing emails, fraudsters can lock the computers of regular users and then demand a payment to free the computers. This is known as ransomware. It might stop users from using the entire functionality of the device, from launching applications, from encrypting files, etc. Ransomware was employed in the well-known WannaCry outbreak to extract money from victims [13].

4.4. Denial of Service Attacks

When a malicious attacker floods a website with traffic, denial of service attempts to stop authorized users from obtaining services or information from that website. The prevention of distributed denial of service (DDoS) is more challenging. This is due to the fact that it originates from numerous computers that are dispersed over the globe; the collection of these infected machines is known as a botnet. For instance, a DDoS attack once targeted Dyn, a US domain name server management service provider, bringing down numerous websites on the US East Coast [14].

4.5. APT (Advanced Persistent Threat)

Advanced persistent threats are covert cyberattacks in which people or organizations acquire unauthorized access to a network and evade detection for a long time [15]. The repercussions of these attacks are severe and include: theft of intellectual property (such as trade secrets or patents), compromising of sensitive information (such as private employee and user data), harm to vital organizational infrastructure, etc.

4.6. Insider threats

In the Big Data era, computer networks are especially susceptible to intrusions by malevolent insiders who already have privileged access to organizational systems [16]. Since insiders can harm a network without entering it, insider attacks can be challenging to identify and defend against. Compromise of a company's internal management system passwords is one example of a human-made activity that could have major repercussions for the organization.

5. Protection measures for security issues

As a result, we may respond to some of the issues and risks that exist in computer networks in the contemporary context of big data by taking the necessary security protection measures. These measures primarily focus on the following aspects:

5.1. Monitoring computer network systems and using threat intelligence

Threats and vulnerabilities can be found using intrusion detection technology and firewall technology, and appropriate defensive actions can be taken. Make that computer network managers are capable of automatically detecting risks, comprehending their context, and understanding the consequences of those threats [17].

DOI: 10.54254/2755-2721/4/2023326

5.2. Clear access controls and the use of strong authentication

Access rights for each position in the network system are subject to strict access control and log management. Furthermore, for particularly sensitive applications or systems, such as human resources, accounting, user data systems, etc., security mandates the use of stronger authentication techniques, such as strong multi-factor authentication, which combines user IDs and passwords with tokens, smart cards, or fingerprint readers.

5.3. Methods of isolating the network

Using subnets inside the same network or by establishing virtual local area networks (VLANs), it is possible to divide the network into zones according to security requirements, which is a crucial step in preventing network security threats [18]. To accomplish this, all requests can be routed through a transparent proxy, which can also be used to monitor and control user behavior and defend against threats like APT attacks and infiltration.

5.4. Conducting regular security scans and software updates

In order to ensure that all software is updated, vulnerability scanning technologies can be used to scan your organization's IT infrastructure and update vulnerable software versions, including operating systems and antivirus programs. This is so that security flaws can usually be fixed when a new version of software is published.

5.5. Implementing internal staff security training

Employees within a corporation are likely the weakest link in data protection. Assuring that insiders in the computer network are aware of cyber security, such as typical phishing attempts and cyber fraud, can help them see threats when using the network on a daily basis. Additionally, emerging approaches like behavioral analysis can be used to spot internal users' suspicious or odd behavior, which can help spot internal attacks [19].

6. Conclusion

Network information security has grown to be a critical issue that needs to be addressed with the introduction of big data. This paper's main topic is the study of computer network information security in the big data era. It examines the traits of big data-era computer network information security as well as the big data information security protection technologies that are currently available and the issues that are currently present in the information security environment. It then makes some concrete protection recommendations for the issues that are currently present. Network situational awareness, vulnerability analysis, intrusion detection and firewall technology, and identity authentication are examples of network information security technologies in the big data era. The universality, suddenness, secrecy, and intelligence are specific traits of computer network information security.

The main problems with today's network information security are phishing attacks, computer viruses, ransomware, denial of service attacks, APT attacks, and threats from within the network. The primary countermeasures for these current issues include the creation of network monitoring and threat intelligence systems, the use of access control and authentication technologies, network isolation techniques, routine software scanning and updating, the organization of internal staff security training, etc. We can fully comprehend the state of computer network information security now and its characteristics thanks to the aforementioned research. We can also analyze contemporary information security issues. and The research indicated above has allowed us to completely understand the condition of computer network information security in the Big Data age. Additionally, by examining current information security issues and associated protection technologies, we can help pertinent computer security researchers analyze and comprehend the pulse and ideas of information security protection in the Big Data environment, allowing them to offer more thorough and accurate information security protection solutions.

DOI: 10.54254/2755-2721/4/2023326

The Big Data era's concerns with computer network information security are always changing since, as is clear, security assault and defense is a dynamic process. This thesis still has many flaws because of the author's constrained research time and expertise. Beginning with the fact that the literature analysis is unable to give a thorough overview of the problems with computer network information security in the big data era, including the innumerable web security vulnerabilities like SQL injection and XSS assaults, etc. Second, current development is not stressed by the examined network information security technologies and defensive techniques. For instance, conventional assault and defensive techniques have changed as a result of the development of artificial intelligence technology, and this area is currently the focus of study for security protection technology. As a result, in the following stage, we intend to methodically summarize the computer network information security challenges in the big data era and create an associated knowledge map that can be dynamically updated. This can aid security researchers in conducting a thorough examination of security issues. Additionally, we intend to pay close attention to the most recent academic studies in network security protection technology, particularly in intelligent security defense technology, to conduct additional research. For example, we may implement automated vulnerability detection using deep learning techniques [20], which can assist us in developing a more effective, intelligent, and automated network security protection system.

References

[1] Liu Yahui, Zhang Tieying, Jin Xiaolong, et al. Personal privacy protection in the era of big data [J]. Computer Research and Development, 2015:1.
[2] Jiao Ruiwen. Talking about information security in the era of big data [J]. Digital Users, 2019(19):4.
[3] Xi Xiaolin. The effectiveness of computer network security technology in the era of big data [J]. Network Security Technology and Application, 2022(4):2.
[4] Yang Bohan. Network security and intelligence analysis based on big data [J]. Modern Information Technology, 2018, 2(7):3.
[5] Fu Yu, Li Hongcheng, Wu Xiaoping, et al. A Review of APT Attack Detection Based on Big Data Analysis [J]. Journal of Communications, 2015, 36(11):2.
[6] Mirsky Y , Lee W . The Creation and Detection of Deepfakes: A Survey[J]. ACM Computing Surveys, 2021, 54(1):2.
[7] Whelan J , Alkemade A, El-Khatib K . Artificial intelligence for intrusion detection systems in Unmanned Aerial Vehicles[J]. Computers & Electrical Engineering, 2022, 99:107784-107785.
[8] ZHANG Wei-da. A Brief Talk on Computer Network Security Technology in the Background of Big Data Era [J]. Digital Technology and Application, 2018, 36(12):3.
[9] Yang Mingxin, Jiang Yuguo, Guo Wendong. Research on Nmap and Distributed Scanning Technology [C]. Proceedings of the Ninth National Conference on Enterprise Informatization and Industrial Engineering. Chinese Institute of Electronics; 2005.
[10] Li Wei, He Xiaokun, Jiang Yun. Research on the linkage between intrusion detection technology and firewall technology [J]. Computer Knowledge and Technology: Academic Edition, 2008, 3(11):2.
[11] Li Xiaoyan. Research on the evolution history and development trend of network trusted identity authentication technology [J]. Information Security and Technology, 2018, 009(011):6-11,18.
[12] Microsoft Digital Defense Report [online]: https://www.microsoft.com/en-us/security/business/security-intelligence-report
[13] WannaCry ransomware attack [online]: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
[14] DDoS attacks on Dyn [online]: https://en.wikipedia.org/wiki/DDoS_attacks_on_Dyn
[15] Guo Nan. Interpretation of Advanced Persistent Threats [J]. Information Security and Communication Secrecy, 2014(11):2.
[16] Tian Zhihui. On Computer Network Security and Its Countermeasures [J]. Computer Programming Skills and Maintenance, 2016(17):2.

DOI: 10.54254/2755-2721/4/2023326

[17] Yang Qing. Detection of abnormal network traffic based on big data analysis [J]. Mechanical Design and Manufacturing Engineering, 2018, 47(11):4.
[18] Wang Hui. The Practical Application of Virtual Local Area Network (VLAN) [J]. Heilongjiang Science and Technology Information, 2011, 000(036):108-108.
[19] LI Ying, LUO Yi, ZHAN Xu, et al. A new generation of WLAN network monitoring and user behavior analysis system [J]. Journal of Chongqing University of Posts and Telecommunications: Natural Science Edition, 2010 , 22(4):501-506.
[20] Gu Mianxue, Sun Hongyu, Han Dan, et al. Software security vulnerability mining based on deep learning [J]. Computer Research and Development, 2021, 58(10):23.