Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

15th June 2024. Vol. 3. No. 3; e-ISSN: 2808-4519

Latest Challenges and Trends in Network Security: Facing Cyber Threats in the Digital Era

Akhmad Galib Andreas[1], Muhlis Tahir[2], Charlista Angel Puspita Gozal [3], Sophia[4], Alfed Mubarok[5], Ahmad Zahrial[6], Selvira Pramesti Cahyani[7]

[1, 2, 3, 4, 5, 6, 7]Pendidikan Informatika, Universitas Trunojoyo Madura, Indonesia
akhmadgalib29@gmail.com[1], muhlis.tahir@trunojoyo.ac.id[2], charlistaghozal@gmail.com[3], sofiyahsofi74@gmail.com[4], alfedmubarok@gmail.com[5], ahmadzahrial25@gmail.com[6], selvirapramesti09@gmail.com[7]

Abstract

In the ever-growing digital era, network security is becoming increasingly important considering the increasing adoption of information technology and the internet. Cyber threats such as hacking attacks, data theft, ransomware and identity theft are lurking threats for both companies and individuals. To overcome these challenges, effective security strategies are needed to protect networks and data from cyberattacks. This research uses a qualitative approach with literature studies to understand the perceptions, views and solutions of experts in the field of network security. The research results show that training, education, cyber security strategies and cross-sector collaboration are the keys to facing cyber threats and maintaining data integrity in an ever-evolving digital environment.

Keywords: Cyber threats, Network security, Literature study.

1. Introduction

In The digital era continues to develop, network security challenges are increasingly complex and diverse. Cyber threats such as hacking attacks, data theft, and malware are lurking threats for both large companies and individuals. Understanding and overcoming these challenges is critical to maintaining the integrity, confidentiality, and availability of data in computer networks.

With the rapid growth of information and communications technology (ICT), computer networks have become the backbone for business operations, public services, and social interactions. However, along with the benefits, the presence of this network also carries risks that cannot be ignored. Attacks on network infrastructure and data have become a real threat to organizations and individuals around the world.

This phenomenon is driven by a variety of factors, including the complexity of network infrastructure, the rapid growth of connected devices (IoT), and the increasingly sophisticated methods used by cybercriminals. Moreover, the need for data availability and uninterrupted connectivity places additional pressure on network security aspects [1], [2].

According to ISO (International Organization for Standardization), ISO/IEC 27032, citing various sources, information security or cyber security refers to maintaining the confidentiality, integrity and availability of information in cyberspace. Cyberspace refers to a complex environment and is the result of interactions between humans, software and Internet services through the use of various technological devices and various network connections and informal environments [3].

In the case of Indonesia, according to the BSSN (National Cyber and Crypto Agency), from January to August 2020, almost 190 million cyberattack attempts occurred in Indonesia, an increase of four compared to the previous year according to the 2019 period or around 39 million. Many sites also believe that cyberattacks will continue in 2021 [4].

One of the most important factors influencing cyber security management is how to understand threats in the cyber world and then find solutions. Without proper cybersecurity measures, the likelihood of threats will increase. The main challenges currently are strengthening the institutions responsible for cyber security, the lack of a legal basis for cyber security, and the lack of skilled personnel and cooperation at home and abroad [5].

In facing this challenge, the solutions offered must include a holistic and proactive approach. First, there is a need to increase awareness of information security at all levels, from end users to network administrators. Training and education on good security practices is key to building a strong defense against cyberattacks.

In addition, the implementation of sophisticated security technology is also needed to detect and prevent emerging threats. This includes the use of robust firewalls, intrusion detection systems (IDS), data encryption, and AI-based security solutions that can identify suspicious behavioral patterns.

The importance of collaboration between government, industry and academic institutions cannot be understated either. Cross-sector cooperation in sharing information about threats and best practices can strengthen overall cyber defense.

Much research and effort has been made to explore and overcome network security challenges in this digital era. A number of studies have focused on developing stronger encryption algorithms and techniques to protect sensitive data. Other work explores new ways to detect cyberattacks quickly and effectively, including the use of big data analytics and artificial intelligence.

Additionally, there are efforts being made to develop more stringent security standards and security frameworks that can be widely adopted by organizations. Work on law and policy is also critical to crafting effective regulations to protect data security and privacy.

By referring to previous research and projects, this research aims to contribute to understanding, identifying and overcoming existing network security challenges, as well as facing future trends and threats in the ever-changing digital era.

2. Theoretical Basis

Network security is the practice of protecting the integrity, confidentiality, and availability of network information and resources. It involves implementing security measures to prevent unauthorized access, misuse, modification, or denial of service in network systems [6].

In the digital era, network security challenges are increasingly complex and diverse. Some of the main challenges include:

1. Cyber Attacks: Cyberattacks such as hacking, phishing, ransomware, and DDoS (Distributed Denial of Service) continue to grow in technique and intensity [7].
2. Data Theft: Sensitive corporate and individual data is a prime target for cybercriminals, which can cause financial and reputational losses [8].
3. Increased Use of IoT Technology: As more and more devices are connected to the internet, the risk of attacks on IoT (Internet of Things) devices is also increasing [9].
4. Lack of Awareness and Training: Many organizations still lack adequate training and education regarding cybersecurity practices to their employees [10]

Some of the latest trends that are being focused on in network security include [11], [12], [13], [14], [15]:

1. Application of AI and Machine Learning: Artificial intelligence and machine learning technologies are used to detect and respond to threats more quickly and efficiently.
2. Zero Trust Architecture: This approach emphasizes that no user or device is automatically trusted, and all access must be verified at all times.
3. Use of Blockchain: Blockchain is used to ensure data integrity and prevent falsification of information in the network.
4. Cloud Security: With more and more companies adopting cloud services, data and application security in the cloud is becoming a top priority.

To face existing challenges and threats, some effective strategies include [16], [17], [18]:

1. Education and Training: Increase employee awareness of cybersecurity practices and provide ongoing training.
2. Cross-Sector Collaboration: Collaboration between various sectors of industry, government, and academia to develop and share security solutions.
3. Implementation of the Latest Security Technologies: Adopt the latest technologies such as AI, blockchain, and encryption to strengthen network defenses.
4. Strong Security Policy: Develop a clear and comprehensive security policy that covers all operational aspects of the organization.

3. Research methods

3.1. Research Stages

This research aims to investigate the latest challenges and trends in network security through a qualitative approach using literature studies. The focus is to deeply understand the perceptions, views and solutions that have been proposed by experts in the field of network security [19], [20], [21], [22].

The following are the stages that must be carried out in this research:

1. Identify Research Topics
   The initial stage is to identify research topics that are relevant to network security. This involves a deep understanding of key issues in the field of network security, such as hacking attacks, data theft and mitigation efforts.
2. Selection of Literary Sources Data collection
   Once the research topic is determined, the next step is to select relevant literature sources. These literature sources can be in the form of scientific journals, books, research reports, and conference articles that have the credibility and novelty of the desired information. The literature sources used include Google Scholar, Semantic Scholar, Garuda.
3. Data collection
   Data will be collected through a systematic and in-depth literature search using academic databases and digital libraries. This process involves searching for keywords, selecting inclusion and exclusion criteria, and content analysis to find the literature most relevant to the research topic. The keywords used include "Network Security Challenges", "Latest Network Security Trends", and "Cyber Threats".
4. Data analysis

The data collected will be analyzed qualitatively using content analysis techniques. This involves identifying themes, patterns, and trends that emerge from the literature investigated. This analysis helps in understanding the views and solutions proposed by experts in the field of network security.

5. Interpretation of Results
   The analysis results will be interpreted to produce a deep understanding of current challenges and trends in network security. The implications of the research findings will be discussed in the context of recent developments in information and communications technology and their impact on cyber security practices.
   The research stages can be presented as in Figure 1 below:

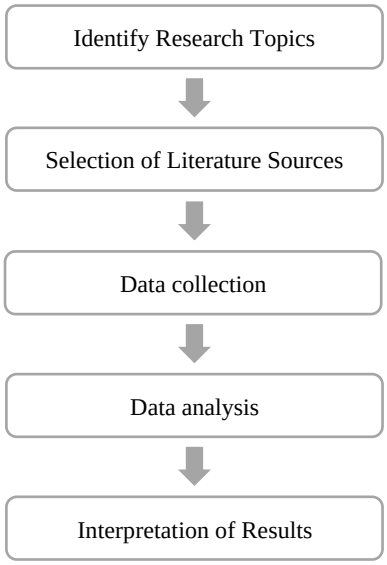

Fig. 1: Research Stages

3.2. Network Security

In this digital era, everyone cannot be separated from the existence of a network, starting from using the network on a cellphone, laptop or computer. Having a network makes it easier for everyone to do various things, from studying, working or even carrying out daily activities. However, along with the development of computer networks, there are still problems with network security. Network security is the process of analyzing and preventing unauthorized network use from intruders who intend to access any of our computer network systems. A network that has been accessed by an intruder can be dangerous because the intruder can misuse our data or computer.

3.3. Cyber Crime Threats

Cybercrime is a criminal act using computer technology individually or in groups with the aim of attacking other computer security systems for certain benefits. Cybercrime is based on various things such as need or just for self-satisfaction. The existence of cybercrime can cause losses to various parties depending on the party attacked, starting from individuals, groups, politics, or a country. An example of cybercrime that we often encounter is the rise of phishing using link messages, or disguised applications sent to someone via WhatsApp social media.

4. Results and Discussion

4.1. Cyber Crime Threats

The emergence of cybercrime began in 1988. At that time, this crime was known as a cyberattack. During this time, the author developed a worm or virus that attacked computers and disabled a total of about 10% of computers connected to the Internet throughout the world.

Cybercrime is an activity or event involving computer technology where a person obtains a profit by causing harm to another party. Cybercrime is also a computer crime committed by an individual or group of people who attack a computer security system or the data contained therein. These crimes are committed for a variety of reasons, ranging from self-gratification to crimes that may cause economic or political harm. Examples of cybercrime include cybersecurity threats such as social engineering, exploitation of software vulnerabilities, and network attacks.

In general, cybercrime is a crime committed using computer technology as the main criminal tool. In other words, someone takes advantage of technological advances to commit crimes. Cyberattacks pose a dire threat to many people today, especially entrepreneurs. It is known that many companies around the world experienced financial losses of up to $1 trillion in 2020 due to the coronavirus pandemic when almost all companies implemented work from home (WFH) policies, which resulted in the relaxation of the rules. digital security.According to a new report from the Center for Strategic and International Studies (CSIS) and McAfee Cybersecurity, the estimated loss of $945 billion is almost double the financial loss due to cybercrime, which was $500 billion in 2018.

Based on a study by the Cyber Crime Directorate (Dittipidsiber) Bareskrim Polri, Indonesia recorded 90 million cases of cyber attacks and according to the Financial Services Information Exchange and Analysis Center (FS-ISAC), Indonesia is on the list of vulnerable countries. against cybercrime attacks. Indonesia itself is ranked 9th. The Covid-19 pandemic is the main topic in cyber security trends. Hackers took advantage of the riots by launching attacks ranging from phishing to ransomware, breaking into the data of 91 million users of the online shopping site Tokopedia, and exposing the data of 1.2 million users of the Bhinneka site.

Indonesia has also been impacted by global cybersecurity cases such as coronavirus ransomware, Covidlock malware, Border Gateway Protocol hacks, Draytek Vigor router vulnerabilities, remote code execution in several product versions of the Windows operating system, and arbitrary code execution vulnerabilities across the Google Android operating system. . Solar Winds Orion platform product.

The pandemic period has also become an easy target for hackers who continue to try to penetrate company security systems because of the intensive use of the Internet when almost everyone is working from home. BSSN data shows that the most attacks were recorded in March 2020, with 22 cyberattacks occurring during the COVID-19 pandemic. These attacks include various types of attacks including HawkEye Reborn Trojan, Blackwater Malware, BlackNET RAT, DanaBot Banking Trojan, Spynote RAT, Netwalker Ransomware, Cerberus Banking Trojan, Ursnif Malware, Adobot Spyware, Metasploit Downloader Trojan, Projectspy Spyware, Anubis Banking Trojan. Adware, hidden ads (Android), AhMyth spyware, Metasploit, Xerxes Bot and Covid19 tracking applications

4.2. Latest Trends in Network Security

The large number of network security cases in the world makes everyone alert. Many digital products are starting to tighten their security to protect data and consumer satisfaction. There are also antivirus companies to protect devices from unknown cybe attacks. Apart from that, currently there are many cyberattacks from various directions, including social media sending messages such as email or other message senders, the need for knowledge to avoid this is very necessary to keep the information we have on computers or networks safe.

4.3. Network Security Challenges

Current challenges in strengthening cybersecurity include: Lack of availability of technology experts and technical security experts to design and implement cybersecurity strategies. This threat arises from the cross-border nature of cyber security, which means that countries with weak cyber security resilience strategies can endanger the cyber security of other countries. The use of anonymization tools, for example to block currency chains or encryption, in cybercrime further complicates policymaking.

The emergence of new technologies and systems requires regular monitoring system updates from time to time. There are new types of telecommunications service providers, often based abroad, that require different treatment than traditional telecommunications companies. New forms of cybercrime such as ransomware, identity theft, grooming, and cyber sexual harassment. Due to the lack of international rules and regulations governing state behavior, we have to deal with cyber attacks and other forms of interstate conflict.

One of the things that answers the challenge of network security is the need for us to have a cyber security strategy. A cybersecurity strategy is a set of actions, policies, and practices designed to protect computer systems, networks, software, and data from cyberattacks and other security threats. Cybersecurity strategies are often holistic and include multiple approaches to containing threats and responding to potential attacks.

5. Conclusion

From the results of this research, it can be concluded that network security has a very vital role in the current digital era. Diverse cyber threats require an effective cyber security strategy to protect data and systems from attacks that could threaten the integrity and availability of information. Training, education, application of advanced security technology, and cross-sector cooperation are key factors in strengthening overall cyber defense. A deep understanding of existing threats and implementing appropriate security strategies is an important foundation for organizations and individuals in maintaining data security and integrity in an ever-evolving digital environment. With awareness of the importance of cyber security, investment in cutting-edge security technology, and collaboration between stakeholders, it is hoped that we can create a digital environment that is safe, secure, and able to face network security challenges more effectively in the future.

References

[1] M. O. Hoshmand and S. Ratnawati, "Security Analysis of Information Technology Infrastructure in Facing Cybersecurity Threats," vol. 5, no. 2, 2023.
[2] R. A. Pulungan, "Network Security Analysis in Industrial Control Systems".
[3] A. Sephira and M. H. Abrar, "CYBER SECURITY ANALYSIS IN THE DIGITAL ERA 'CHALLENGES AND SECURITY STRATEGIES'".
[4] D. R. Yuniarti, H. F. Alfarizy, Z. Siallagan, and M. W. Rizkyanfi, "ANALYSIS OF POTENTIAL AND CYBER CRIME PREVENTION STRATEGIES IN LOGISTICS SYSTEMS IN THE DIGITAL ERA," *J. Logist Business. And Supply Chain BLOGCHAIN*, vol. 3, no. 1, pp. 23–32, Jun. 2023, doi: 10.55122/blogchain.v3i1.714.
[5] Stallings, W., & Brown, L. (2018). Computer Security: Principles and Practice. Pearson.
[6] Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.
[7] S. A. M. Babys, "CYBER WAR THREAT IN THE DIGITAL ERA AND INDONESIAN NATIONAL SECURITY SOLUTIONS," vol. 3, no. 1, 2021.
[8] A. Bustami and S. Bahri, "Threats, Attacks and Protective Measures in Network Security or Information Systems: Systematic Review," *UNISTEK*, vol. 7, no. 2, pp. 59–70, Aug. 2020, doi: 10.33592/unistek.v7i2.645.
[9] Laudon, K. C., & Laudon, J. P. (2016). Management Information Systems: Managing the Digital Firm. Pearson.
[10] N. I. Putri, "Computer Network Security in the Big Data Era," *J. Sist. Inf.*, vol. 02.

[11] F.jauhari and M. I. Wahyuddin, "COMPUTER NETWORK SECURITY IN ELECTRONIC GOVERNMENT SYSTEMS," 2008.
[12] E. Susanto, Lady Antira, K. Kevin, E. Stanzah, and A. A. Majid, "CYBER SECURITY MANAGEMENT IN THE DIGITAL ERA," *J. Bus. Entrep.*, vol. 11, no. 1, p. 23, Jun. 2023, doi: 10.46273/jobe.v11i1.365.
[13] I. E. Maulani, T. Herdianto, D. F. Syawaludin, and M. O. Laksana, "APPLICATION OF BLOCKCHAIN TECHNOLOGY IN INFORMATION SECURITY SYSTEMS".
[14] Northcutt, S. (2009). The Security+ Guide to Network Security Fundamentals. Cengage Learning.
[15] M. Machlul, "Improving the Quality of Human Resources through Cyber Security Training for East Java Regional Police Members," *Parta J. Service. To. Masy.*, vol. 4, no. 2, pp. 150–155, Jan. 2024, doi: 10.38043/parta.v4i2.4655.
[16] F. Indah, A. Sidabutar, and N. Annisa, "The Role of Cyber Security in the Security of Indonesian Population Data (Case Study: Hacker Bjorka)," vol. 1, no. 1, 2022.
[17] M. I. T. Dwikoryanto and Y. A. Arifianto, "Synergy of Pancasila Education and Christian Education in Reducing Cyber Bullying in the Digital Era," vol. 4, no. 1, 2022.
[18] Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W.W. Norton & Company.
[19] Kshetri, N. (2017). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89.
[20] Chintya Pradilla Putri, Widya Anggraini, Yuda Mahendra Hasibuan, and N. Nurbaiti, "Cyber Security Strategy: Scope of Cooperation in Facing Cyber Threats," *INSOLOGY J. Science And Technology.*, vol. 2, no. 6, pp. 1124–1130, Dec. 2023, doi: 10.55123/insologi.v2i6.2847.
[21] Chio, C., & Freeman, D. (2018). Machine Learning and Security: Protecting Systems with Data and Algorithms. O'Reilly Media.
[22] M. Hafid, F. Z. Firjatullah, and B. W. Pamungkaz, "Challenges of Facing Cyber Crime in Community and State Life," vol. 7, 2023.