International Journal of Education and Life Sciences (IJELS)
Vol. 2, No. 11, 2024 : 1363-1372

Computer Network Design and Network Security System Development Computers in the Age of Big Data

Dwi Fahrulrezza, Muhamad Jaky Jamal,Nova Rahmad Prasetya, Emi Sita Eriana, Fajar Haditio

Universitas Pamulang

Corresponding Author: Dwi Fahrulrezza: Dwifahreza67@gmail.com

A R T I C L E I N F O

Keywords: Network, Big Data, System, Network Security, Computer

Received : 6, September
Revised : 16, October
Accepted: 18, November

A B S T R A C T

The proliferation of *big data* has raised new challenges in terms of network security. This research proposes a network architecture inspired by the concept of *software-defined networking* (SDN) to provide high flexibility and scalability in the face of exponential data growth. In addition, an artificial intelligence-based security system is developed to detect increasingly sophisticated threats. The test results show that the designed network architecture is able to improve system performance and reliability, while the security system succeeds in reducing the false detection rate and increasing the intrusion detection rate. This research is expected to serve as a foundation for the development of a more secure and efficient network infrastructure in the *big data* era.

INTRODUCTION

Computer network technology is currently developing at an accelerating rate in tandem with societal demands, particularly those of educational institutions. In particular, services that employ computer networks are highly helpful when it comes to using the internet to manage information so that work becomes more efficient. Two or more computers connected by wired or wireless transmission medium form a computer network. If two computer units can share a resource, exchange data or information, and use hardware or software that is part of the same network, then they are considered connected. Small area computer networks include those found in homes, buildings, schools, and campuses. Generally speaking, a computer network is a collection of computers that are connected to one another. In the sector, a lot of information is extremely sensitive because it cannot be comprehended by unrelated parties or it may create irreversible damage. The great level of confidentiality of computer data is the exact reason why some criminals consider committing crimes. and always hope to gain some benefits from computer network security vulnerabilities. Computer network security technology is constantly evolving, and the criminal technology of these criminals is also constantly evolving.

Network security cannot be ensured since even some criminal technology is too advanced for computer specialists. Computer network security crimes are becoming more frequent because the evidence used in computer crime cases is hard to interpret. In order to reduce the likelihood of computer crime, it is imperative that significant efforts be made to prevent computer network security. There are four key components that make up computer network security: shared resources, network infrastructure, software, and Internet of Things services. The International Organization for Standardization defines computer network security as safeguarding the computer system's data, software, and hardware from security holes due to accidental or malicious reasons, so that the computer system continues to operate reliably, and computer services are also in order. For some reason, they carry out intrusions that can harm the owners of servers and computer networks. They use a variety of computer network attacks with tools that are made independently or that already exist in the market. The sophistication of attacks and tools on computer networks is inversely proportional to knowledge about intrusion on computer networks.

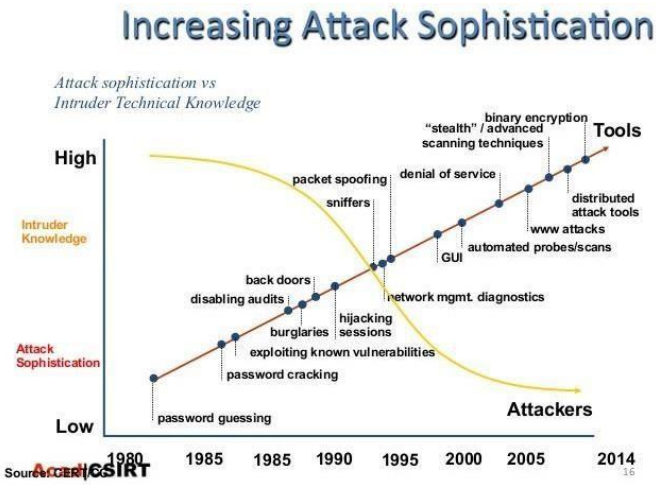


Fig. 1 Attack sophistication vs knowledge of how to infiltrate

The main effect of computer network attacks is slow internet access. In addition, for very dangerous types of network attacks, it can result in data corruption on the server, so this is very detrimental to users or end users who are accessing. Damaging, disrupting, stealing data, and anything that harms the server owner on a computer network is an illegal act and can be legally sanctioned in court. Fighting internet crime has become a major portion of law enforcement and intelligence agencies, both national and international, without exception business practitioners, to customers, and end users. Generally, internet crime starts with exploiting hosts and computer networks so that intruders come across networks, especially TCP/IP-based networks. More specifically, network forensics is the activity of capturing, recording, and analyzing events on computer networks to find the source of security attacks or other problematic events. The power of Forensics is that it enables the analysis and retrieval of facts and events from the environment, as facts may be hidden. Security is often Most firms consider it an afterthought. The use of inappropriate threat detection techniques and security procedures in data protection is the primary cause of this, which can result in security failures. Most firms tend to regard security as an afterthought. Because it is brought on by the application of inappropriate threat detection techniques and security procedures in data protection, it might result in security failures. Rahman and Loukaka (2017). It is preferable to establish security methods from the beginning rather than "adding security to an already complex data environment as an afterthought" (B. Duncan 2018). This is because firms with big data environments should not approach security as secondary. Businesses that have used privacy and security measures in the creation and application

.

Theory Review

A. Computer Network

A computer network is an operating system consisting of several computers and other network devices that work together in achieving the same goal. (Pelealu, Wonggo, and Kembuan 2020). A computer network is a relationship of two or more nodes whose main purpose is to exchange data. Computer networks can connect with each other using communication media, so that they can share data, information, programs, and hardware (printers, hard drives, webcams). According to (Tomi Tristono 2013)(Tomi Tristono 2013), a computer network is a group of many computers that are separate but interconnected in carrying out their duties. Two computers, for example, are said to be connected if both can exchange information.

B. Spyware and Spam

Emails are a more popular method of communication in the typical sense. Email is crucial for working on projects, especially in a variety of occupations. Because of this, a lot of crooks want to exploit email to steal users' privacy or for other illicit activities. By include spam in emails they send, they are primarily pressuring users to accept it. Information loss will occur if people click on or download the special software they installed if they don't check the veracity of these emails..

C. Hacker Attacks and Threats

Hackers refer to a group of people with high intelligence and ability, who

familiar with computer knowledge and very good at computer network security (Okafor, Onwuka, and Okonkwor 2021).. Compared with ordinary people, hackers show fear to users. Hackers can choose destructive attacks and non-destructive attacks if they want to fulfill their own needs through computer networks. Destructive attacks, such as destroying the user's system so that the computer is completely unusable. A non-destructive attack means that hackers only take the information they need without affecting the user's normal use. Common hackers use attack means: Trojan horse attacks, phishing attacks against websites, email attacks and so on.

D. Big Data and Organizational Security Concerns Prior research has noted potential privacy and security concerns with large data (Saraladevi et al. 2015). For instance, privacy-related concerns have been brought up regarding how companies get confidential and sensitive data n(Mennecke and others, 2014). However, there are other concerns with large data security outside data privacy. Because more data is being gathered and stored, a business is also more susceptible to other security risks and cyberattacks. To prevent undesired security breaches, such as disclosing private information to unauthorized parties, security

measures must be appropriately implemented in businesses with big data capabilities. In the absence of strong security measures, it can, Without effective security mechanisms, it can have several impacts on the organization, including reputational damage and financial loss. (Lee 2017)also argues that "weak security creates user resistance to big data adoption". This resistance to big data solution adoption is also supported by the findings of surveys conducted by several marketing research and technology consulting firms. Consistently, security and privacy factors are cited as one of the major barrier factors for the adoption of big data solutions in organizations. (Moorthy et al. 2015).

E. Big data is defined as high volume, high velocity, and high diversity information that necessitates novel information processing techniques in order to get insights and support decision-making (Gandomi and Haider 2015). Generally speaking, big data is defined by six qualities, or what are known as the 6Vs. These aspects are the fundamental features of big data in general.Big data can be described as high volume, high velocity, and high variety information that demands innovative forms of information processing to obtain

insights and for decision making (Gandomi and Haider 2015). Typically, big data is characterized by 6 traits, commonly referred to as 6Vs, which are the basic characteristics of big data, in general.

Fig. 2 6V of Big Data

However, data is classified as big data as long as it meets the first 3Vs of volume, velocity, variety (Adam et al. 2017). Big data technology can be described as a tool or technology used to efficiently process data that has been classified as big data. Some big data technologies include, Apache Hadoop (Zaharia et al. 2016)Apache Spark (Vavilapalli and Murthy, AC 2013).. In the section on big data characteristics have been described, namely 6V.

METHODOLOGY

Researchers employed the Network Development Life Cycle (NDLC) model development approach for system development in this study; installation and monitoring are not specifically done. The foundation of the computer network design process is NDLC. The development process cycle or computer network system is defined by the NDLC paradigm. Cycle is a term used to describe the network system development life cycle that specifically explains every step and procedure involved in the ongoing creation of a network system (Kamu et al. 2022). The NDLC has the following stages: Evaluation: Needs analysis, problem analysis, user desire analysis, and network topology analysis are conducted at the first step. At this point, the methods are as follows: a. Interview b. Direct field survey c. advance.

2. Monitoring: Monitoring activities are carried out after implementation, so that the network computer and communication can run in accordance with the wishes and initial goals of the user at the initial stage of analysis.
3. Management: Management or organization, one that is of particular concern

is a Policy problem, policies need to be made to create or regulate so that the system that has been built can run well for a long time and the Reliability element is maintained. Policy will depend on the management level policy and business strategy of the company. IT as much as possible must be able to support or aligmnet with the company's business strategy.

DISCUSSION

The authors of this study employed the six-stage Network Development Life Cycle (NDLC) system development process, which includes the following stages: analysis, design, prototype simulation, implementation, monitoring, and management. Nevertheless, the scope of this study is restricted to the prototype simulation phase. Utilizing a specialized network simulator application, computer network design requires a minimum of one access point, a minimum of one modem, a router, a PC server, transmission media, the ability to connect to WiFi, an operating system (OS), the TCP/IP protocol, and an IP address division.

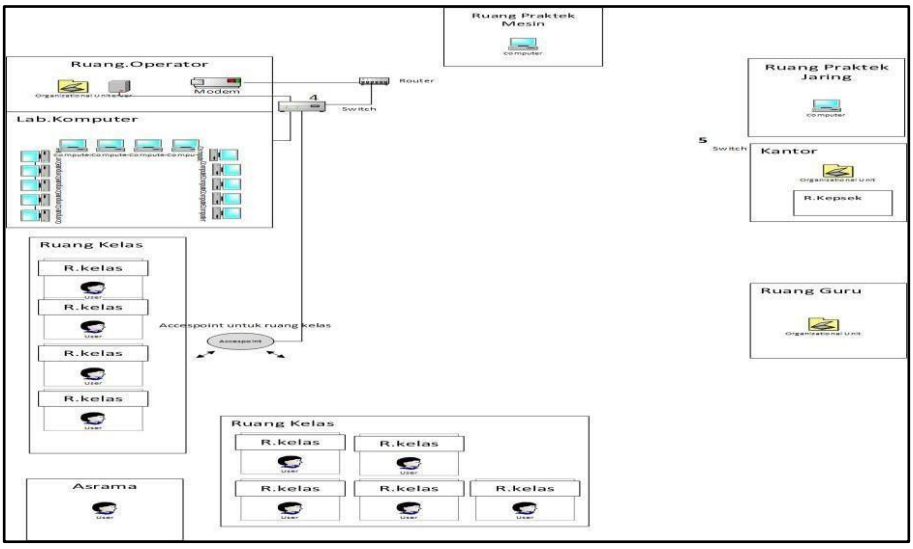
Although computer technology is always evolving, hackers and criminals are also always learning new things, thus we must not stop researching the advancements in computer network security technology. Protective technology needs to keep up with the rate at which cybercriminals pick up viruses. As was previously said, one of the most commonly cited issues in computer network security is information security flaws in data encryption technology" It is more harder to steal user information thanks to data encryption technology. A technology known as data encryption uses specific data processing methods to

hide or encrypt data so that computer network users would not be able to decipher it. Data encryption comes in two flavors: public key encryption and private key encryption. The use of public key encryption is It was developed relatively late and is more secure than private key encryption. The two stages of private key encryption are encryption and decryption. Because the processes of encryption and decryption are linked, data security is safeguarded.

Private key encryption is not limited to users; anybody can set it up and use it. Compared to public key encryption, key encryption is easier to deploy and decrypts data faster. It is found that both private key and public key cryptography have distinct advantages when comparing their features. Data encryption should have a stronger impact in private settings. if public key encryption and private key encryption can be used in tandem.. Firewall technology, Firewall is a security technique to protect computer security and prevent computer failure, also belongs to the most commonly used type of computer security measures. Firewalls can be hardware, software, or between two or more computers. Firewalls can provide a more substantive role in protecting computers, as all data streams need to be filtered through the firewall [24]. In general, the firewall has the following functions, the first function, the firewall can prevent other unrelated people from entering the user's personal computer; the second function, even if someone from the outside enters the system, then the firewall can prevent it from approaching the defense facilities; third, the firewall can prevent visiting specific sites due to its ability to filter unwanted addresses and finally, the firewall can prevent visiting specific sites. In essence the computer must provide security monitoring.

Network Requirement Analysis

To support the institution, Computer networks must be carefully planned in order to maximize resource utilization and accomplish the goals and objectives. Given the intricacy of the issues with the administrative system, computer networks are essential.



Network Design

Fig. 3 network design 1

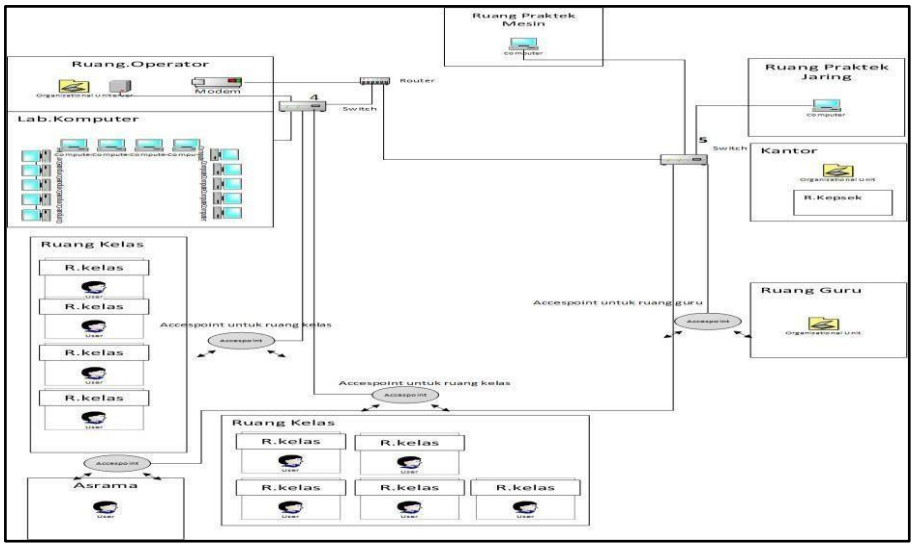


Fig. 4 network design 2

The school employs Telkom Speedy with direct internet via ADSL modem for internet services, as can be demonstrated by the network design drawings in Figures 3 and 4. The figure's numbering provides the following explanation.:

1) Modem installed in the operator room.
2) The router functions as a firewall router as well as in bandwidth management.
3) Server pc in IP Address sharing.
4) The main switch located in the operator's room, server and computer lab, the network will be intended for the operator's room, computer lab and Accespoint for the classroom.
5) Switch two is located in the office room whose network is intended for space

office and principal. And Accespoint for the teacher's room and surrounding classrooms.

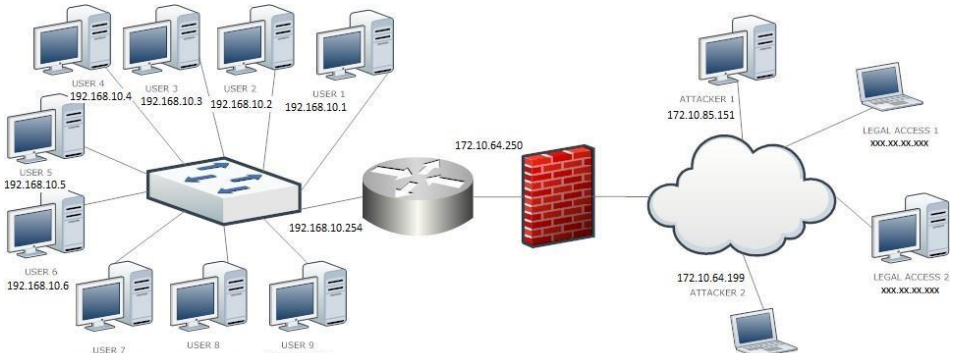


Fig. 5 network topology

The research is shown in Figure 5. Where the user's computer is connected to a star model (star) with a switch then successively connected to a router then a firewall is made as a security system and the last is connected to the internet. The network can be accessed both from inside and outside the computer network.

CONCLUSION

Based on the results of testing and analysis, a computer network security system can be designed using computer network forensic evidence. And after a computer network security system is created, attackers will not be able to carry out attacks in the future using the same method. At least one accesspoint, at least one modem, a router, a PC server, transmission media, the ability to connect to WiFi, an operating system (OS), the use of TCP/IP protocols, and IP address sharing are all required for computer networks. Two computer network model designs are then created based on these minimal requirements.

It is important for all computer users to understand the subject of computer network security. Phishing websites, illicit links, spam, and other issues must be removed from the computer. Never give criminals a chance since doing so is careless and can seriously affect computer security. Furthermore, it is imperative that computer network security technologies continue to advance and decrease illicit aspects as quickly as feasible. Future developments in computer network security technology still have a long way to go. Numerous technological innovations must to be implemented as quickly as feasible, and security precautions ought to be strengthened.

BIBLIOGRAPHY

Adam, Khalid, Mohammed Adam, Ibrahim Fakharaldien, and Jasni Mohamed Zain. 2017. "BigData: Issues, Challenges, Technologies and Methods BigData: Issues, Challenges, Technologies and Methods," no. March.

B. Duncan, M. Whittington and V. Chang. 2018. "Enterprise Security and Privacy: Why Adding IoT and Big Data Makes It So Much More Difficult." *International Conference Engineering Technollogy, ICET 2017*, 1-7.

Gandomi, Amir, and Murtaza Haider. 2015. "Beyond the Hype: Big Data Concepts, Methods, and Analytics." *International Journal of Information Management* 35 (2): 137–44. https://doi.org/10.1016/j.ijinfomgt.2014.10.007.

You, Israel, Mario Tulenan Parinsi, Meikel Wolter Kuhu, and Arther Valentino Mananggel.

2022. "Computer Network Design in Vocational School Using Network Simulator." *International Journal of Information Technology and Education* 2 (1): 22–31. https://doi.org/10.62711/ijite.v2i1.86.

Lee, In. 2017. "Big Data: Dimensions, Evolution, Impacts, and Challenges." *Business Horizons*

60 (3): 293–303. https://doi.org/10.1016/j.bushor.2017.01.004.

Loukaka, Alain, and Shawon S.M. Rahman. 2017. "Discovering New Cyber Protection Approaches from a Security Professional Prospective." *International Journal of Computer Networks and Communications* 9 (4): 13–25. https://doi.org/10.5121/ijcnc.2017.9402.

Mennecke, Brian, Heng Xu, Chuan Hoo Tan, H. Jeff Smith, Malcolm Crompton, Marie Shroff, and Joey F. George. 2014. "Privacy in the Age of Big Data: The Challenges and Opportunities for Privacy Research." *35th International Conference on Information Systems "Building a Better World Through Information Systems", ICIS 2014*, 1-5.

Moorthy, Janakiraman, Rangin Lahiri, Neelanjan Biswas, Dipyaman Sanyal, Jayanthi Ranjan, Krishnadas Nanath, and Pulak Ghosh. 2015. "Big Data: Prospects and Challenges." *Vikalpa* 40 (1): 74–96. https://doi.org/10.1177/0256090915575450.

Okafor, Chika Lilian, Uchenna Paulinus Onwuka, and O R Okonkwor. 2021. "Security Issues and Its Management in Network." *Idosr Journal of Experimental Sciences* 6 (1): 111-17. www.idosr.orgOkaforetal.

Pelealu, Ray R A, Djafar Wonggo, and Olivia Kembuan. 2020. "Design and Implementation of Smk Negeri 1 Tahuna Computer Network." *Jointer* 1 (1): 6. http://jointer.id/index.php/jointer/article/view/4.

Saraladevi, B., N. Pazhaniraja, P. Victer Paul, M. S. Saleem Basha, and P. Dhavachelvan. 2015. "Big Data and Hadoop-A Study in Security Perspective." *Procedia Computer Science* 50: 596-601. https://doi.org/10.1016/j.procs.2015.04.091.

Tomi Tristono, Santi Dwi Nurhumam. 2013. "Computer Network and Internet Design in School." *Agri-Tek* 14 (1): 42-49.

Vavilapalli, VK, and C Douglas Murthy, AC. 2013. "Apache Hadoop Yarn: Yet Another Resource Negotiator Big Data Resources Scheduling." *The 4th Annual Symposium on Cloud Computing*, 1-16. https://dl.acm.org/citation.cfm?id=2523633.

Zaharia, Matei, Reynold S. Xin, Patrick Wendell, Tathagata Das, Michael Armbrust, Ankur Dave, Xiangrui Meng, et al. 2016. "Apache Spark: A Unified Engine for Big Data Processing." *Communications of the ACM* 59 (11): 56–65. https://doi.org/10.1145/2934664.