JURNAL EMACS
e-ISSN: 2686-2573
[Engineering, MAthematics and Computer Science] Vol.4 No.3 September 2022: 109-112 DOI: 10.21512/emacsjournal.v4i3.8634

The Role of Network Security in Class Conference During COVID-19 Pandemic

Ivan Sebastian Edbert[1*], Fidelson Tanzil[2], Julio Pramaitama[3], Kevin Tio[4], Muhammad Rizal Rizky[5], Alvina Aulia[6]

[1,2,3,4,5,6] Computer Science Department, School of Computer Science,
Bina Nusantara University,
Jakarta, Indonesia 11480
ivan.edbert@binus.ac.id; Fidelson.tanzil@binus.ac.id; julio.pramaitama@binus.ac.id;
kevin.tio@binus.ac.id; muhammad.naufal015@binus.ac.id; aaulia@binus.edu

*Correspondence: ivan.edbert@binus.ac.id

Abstract – *Security is crucial for the network. But there are still system leaks, especially in class conferences during the pandemic. Because of a lot of data exchange and data entry, some viruses are difficult to identify. So, the role of network security is vital. Many viruses spread through links, and others can access cases of misuse of links; the issue is called Zoom bombing. So, from managing the instability of data in and out of conference classes during this pandemic, many activities are carried out online that awareness of more comprehensive network security. With the COVID-19 pandemic, class conferences are prevalent in today's world. Millions of people use it for various reasons, and one of them is for education. However, there are issues related to the network's security where users' data was stolen and impersonated or network trafficking, which will cause fault and disruption in the network. This research have 3 methodologies include Systematic Literature Review, Research Questions (identify the focus of the literature review, which helps process the data more clearly), Result Finding (the study of an existing paper with specific keywords to answer the research questions). As the result, it can be concluded that there are many ways to prevent attacks by improving the network's security such as network security defense mechanisms and firewall. So that everything can be petrified in terms of comfort in meet conferences so that class conferences activities can run safely.*

Keywords: *Network Security; Conference Class; Cyber Attack COVID-19; Zoom Bombing*

I. INTRODUCTION

The COVID-19 pandemic has impacted every aspect of life. These are shown by how people study, work and socialize. Office workers started to work from home, students began learning from home, and people started socializing through social media through voice or video calls. Most business purposes, academic, and educational use have shifted their activities to online through teleconference. With these activities happening, a lot of data is transferred through the internet. Hence, in this case, security is essential and must be considered. However, many users neglect the importance of safety.

The growth of digital resources has many advantages but also big problems. In 2020, there was an incident where an anonymous showed pornography content to the public when the school activities were ongoing at Daniel Hand High School in Madison, Connecticut. Several countries also reported such incidents throughout the globe. This kind of activity is known as Zoom bombing. Zoom bombing or Zoom raiding is an unwanted, disruptive intrusion during conference calls done by someone intentionally to cause a disturbance. This term is originally derived from the name Zoom, a video conference platform, but it is now used to refer to such phenomena on other video conference platforms.

Network security is considered an act of data protection during transmission through interconnected network groups. The use and popularity of the internet and computer networks have grown over the years, giving great importance to gaining access to digital resources[1]. Classify with the increasing use and popularity of internet resources globally. Today's reality is very connected and complex, using several technologies which will impact the congested

internet network. Cybercriminals are interested in taking control of devices by stealing data from students, workers, business people, and others[2].

The class conference depends on the network, and it is increasingly used because its convenience supports it. The task that makes the network important is its security. Of course, there can also be traffic, but it is crucial if connection problems occur with network or computer resources. The main factor is security, so cyber thieves who arbitrarily stole personal data can't do their actions. To find out where the thief who took the data during class conferences during this pandemic, try to connect to a short router because the farther the router is, the riskier it is for something untoward to happen[3].

In this study, our primary focus is on explaining the importance of security, the role in network security, and the methods we will use, such as mechanisms, benefits, and how network security works. During this COVID-19 pandemic, it was not an obstacle for us to carry out activities. So, with the many activities we run, all of which are online, there is something we need to know in this study that can add to our knowledge. Furthermore, a sense of technological development will continue to develop over time. Therefore, this paper will explain the critical role of network security in the online classes we have been running so far during the pandemic.

II. METHODS

2.1 Systematic Literature Review

Systematic Literature Review (SLR) is a research methodology or specific research and development carried out to describe, identify, evaluate, consolidate, interpret and collect research related to the topic.

This research aims to better understand the context of the topic, the objectives to be taken, and the user's experience in the class conference during the pandemic to get a broad and complete picture of the results.

2.2 Research Questions

Research questions are used to identify the focus of the literature review, which helps process the data more clearly. Table 1 shows the research questions for this research.

Table 1. Research question

No	Research Question	Motivation
1	What is the purpose of a secure network for the class conference?	To identify the definition of a secure network for class conference
2	What kind of method helps increase network security?	To identify methods that increase the network security

2.3 Result Finding

The study of an existing paper with specific keywords to answer the research questions. The keyword used in this study is "network security" AND "class conference." Table II shows the results of the search. Table 2 shows the number of findings from various database journals.

Table 2. Search results on each database journal

No	Database Journal	Number of Articles
1	Scopus	26.232
2	IEEE Xplore	5
3	ScienceDirect	6.908
4	SpringerLink	6.432
Total		39.577

III. RESULTS AND DISCUSSION

3.1 Purpose of Secure Network on Class Conference

Many people ignore the importance of network security because they don't understand how it works and how to prevent it. Cyber-attacks such as data loss and IP Spoofing that leads to impersonation and network trafficking often occur on the non-secured network.

A secure network for class conferences aims to prevent these types of cyber-attacks. During the class conference, cyber-attacks may cause interruption to the ongoing conference room. Therefore, a secure network is an important aspect that must be fulfilled and concerned. Motivating participants related to secure networks can motivate participants who want to keep cyber-attacks secure against class conferences. This purpose is the most commonly used in conference classes for online meetings. The last objective is with lots of activity all online. So, a secure network plays a significant role in maintaining comfort in attending conference classes[4].

3.2 Methods To Increase Network Security

There are many types of network security defense mechanisms:

3.2.1 SDHoneyNet

Software-defined HoneyNet (SDHoneyNet) is a defense mechanism to attract potential attackers[5]. SDHoneyNet is installed on a decoy network by using the assets such as network devices as bait to analyze the attacks. From there, the defender side will gather information about the security threats used by the attackers to prevent future attacks and enhance their security system[6].

3.2.2 Moving Target Defense Mechanism

The Moving Target Defense (MTD) mechanism was designed based on SDN to mitigate crossfire attacks, a sophisticated type of Distributed Denial of Service (DDoS) attack. MTD works before the attack and during the attack. MTD design consists of four modules where each module has its responsibility, such as ICMP monitoring, traceroute profiling, route mutation, and congestion link monitoring. The way MTD works is by tracking the routes and updating the state of the network. Collecting updated information makes it easy to misguide the attackers[7].

3.2.3 CoFence

CoFence is a framework based on collaboration with the NFV domain network, wherein each domain contains an Intrusion Prevention System (IPS) to filter and detect DDoS

attacks. The way it works is by communicating with each other. As a result, the field can handle a large amount of traffic, reducing the attack flows to the targeted network.

3.2.4 Fog computing and Blockchain-based

Technological developments with the arrival of the blockchain have made it an extraordinary, most revolutionary, and continuously evolving thing in recent years. Blockchain is used in money-related exchanges that track transactions and events across the network. Blockchain uses a 256 SHA hash. The Blockchain network can be duplicated to a particular place, for example, in a distribution network capability or service or as a regional or global data exchange system. Fog computing is a modern model offering geographically dispersed end-users latently-aware services. Fog computing includes agility, power, network protocols, and disseminated data analytics[8].

3.2.5 Blockchain Signaling System

Blockchain Signaling System is composed of two components, decentralized application (dApp) and Smart Contracts (SC), where SC helps define how the information is interchanged between autonomous systems while dApp holds the variable on how the independent system communicates with each other[8]. Furthermore, this system can verify the integrity of the attack information, which allows data to be posted to the blockchain and makes the forgery attack (IP Spoofing) impossible[9].

3.2.6 SoftThings

SoftThings is an SDN-based security framework that captures and prevents attacks on IoT devices[10]. The system has several layers: the device layer, SDN controller layer, and SDN master controller layer. This system uses machine learning algorithms at the SDN controller layer to monitor and detect abnormal behaviors of the IoT devices, which will then be reported to the master controller to examine if an attack exists or not.

3.3 The benefit of Ontology Modeling for NSSA

Network Security Situational Awareness (NSSA) is used to monitor the network situation in real-time, issue warnings before potential and malicious network behaviors are out of control and give corresponding countermeasures. The ontology is built based on network security. There are four situation concepts: context, vulnerability, attack, and network flow.

The ontology modeling for NSSA aims to reflect the network security situation of the class conference. Shortly, there will be benefits from this modeling, which can be obtained by avoiding cyber threats, detecting physical information network security attacks, and reducing the vulnerability of Zoom bombing events[11].

3.4 Firewall

A firewall is a network security system that manages network traffic by blocking incoming or outgoing traffic based on ports and IP addresses. A firewall creates a barrier between the network and the internet. A firewall is used in a private network to prevent different kinds of attacks, such as impersonation attacks, which use spoofed IP addresses that lead to data loss and viruses carried by other participants in the conference call[12].

The firewall uses three methods to control incoming and outgoing traffic. The first method is packet filtering, and firewall software creates a predetermined rule to create filters where incoming data is checked by the filter to be determined if it can go through or not. The second method is proxy service, which examines all the applications used for IP packets to verify their authenticity. Proxy services often require the administration to configure their network settings and application to support the proxy being used. The third method is stateful packet inspection. First, all parts of the IP packet are examined to determine whether the request for communication should be accepted or rejected. Then, the requested data proceeds to the screening process to assess the state of each piece of information[13].

3.5 Previous Study

The previous study concluded that the development of security measures such as encryption, intrusion detection, and firewalls had increased urgently, and the continuous change and challenge with new technologies. Maintaining control over how data is used, stored, and shared is difficult, which is why their use of secure protocol will lead end users to protect their home network and institutions to protect their corporate network. All the data that is exchanged will be saved and encrypted to prevent any attacks. A firewall is an example of a secure protocol that helps prevent foreign viruses and plug-ins from attacking the computer and enhances the security and privacy of computer users.

IV. CONCLUSION

COVID-19 has brought many changes to our lives that we must accept and do. Unfortunately, it has become common in this case. Even though the pandemic has become an endemic, activities such as conferences over the air or online classes, conferences with friends, family, or colleagues will be new challenges or problems that may arise. From this research, it can be concluded that there are many ways to prevent attacks by improving the network's security, such as a firewall by filtering traffic on IP addresses which will prevent data loss and impersonation. While Moving Target Defense works by tracking network routes that will help avoid DDoS attacks. So that everything can be petrified in terms of comfort in meet conferences so that class conferences activities can run safely.

REFERENCES

[1]G. Elmer, S. J. Neville, A. Burton, and S. Ward-Kimola, "Zoombombing During a Global Pandemic," *Social Media and Society*, vol. 7, no. 3, 2021, : 10.1177/20563051211035356.

[2]M. Anghel and G.-C. Pereteanu, "CYBER SECURITY APPROACHES IN E-LEARNING," in *INTED2020 Proceedings*, Mar. 2020, vol. 1, pp. 4820–4825. doi: 10.21125/inted.2020.1323.

[3]J. Liu, Z. Tian, R. Zheng, and L. Liu, "A Distance-Based Method for Building an Encrypted Malware

Traffic Identification Framework," *IEEE Access*, vol. 7, pp. 100014–100028, 2019, doi: 10.1109/ACCESS.2019.2930717.

[4]A. M. Gabor, M. C. Popescu, and A. Naaji, "Security Issues Related To E-Learning Education," 2017. [Online]. Available: https://www.researchgate.net/publication/349536752

[5]A. Dahiya, K. Joshi, R. Nandal, R. Yadav, and S. Bal Gupta, "Honeynetbased Defensive mechanism Against DDoS Attacks."

[6]Z. Wang *et al.*, "Honeynet construction based on intrusion detection," Oct. 2019. doi: 10.1145/3331453.3360983.

[7]R. Swami, M. Dave, and V. Ranga, "Software-defined Networking-based DDoS Defense Mechanisms," *ACM Computing Surveys*, vol. 52, no. 2, May 2019, doi: 10.1145/3301614.

[8]P. G. Shynu, V. G. Menon, R. L. Kumar, S. Kadry, and Y. Nam, "Blockchain-Based Secure Healthcare Application for Diabetic-Cardio Disease Prediction in Fog Computing," *IEEE Access*, vol. 9, pp. 45706–45720, 2021, doi: 10.1109/ACCESS.2021.3065440.

[9]B. Rodrigues, E. Scheid, C. Killer, M. Franco, and B. Stiller, "Blockchain Signaling System (BloSS): Cooperative Signaling of Distributed Denial-of-Service Attacks," *Journal of Network and Systems Management*, vol. 28, no. 4, pp. 953–989, Oct. 2020, doi: 10.1007/s10922-020-09559-4.

[10]A. al Hayajneh, M. Z. A. Bhuiyan, and I. McAndrew, "Improving internet of things (IoT) security with software-defined networking (SDN)," *Computers*, vol. 9, no. 1, Mar. 2020, doi: 10.3390/computers9010008.

[11]G. Xu, Y. Cao, Y. Ren, X. Li, and Z. Feng, "Network Security Situation Awareness Based on Semantic Ontology and User-Defined Rules for Internet of Things," *IEEE Access*, vol. 5, pp. 21046–21056, Aug. 2017, doi: 10.1109/ACCESS.2017.2734681.

[12]M. T. Arefin, M. R. Uddin, N. A. Evan, and M. R. Alam, "Enterprise network: Security enhancement and policy management using next-generation firewall (ngfw)," *Lecture Notes on Data Engineering and Communications Technologies*, vol. 66, pp. 753–769, 2021, doi: 10.1007/978-981-16-0965-7_59.

[13]E. by Sabyasachi Pramanik, A. Sharma, S. Bhatia, and D.-N. Le, "An Interdisciplinary Approach to Modern Network Security."