Journal of Integrated and Advanced Engineering (JIAE)
Vol. 1, No. 2, September 2021: 113-122
http://asasijournal.id/index.php/jiae
http://doi.org/10.51662/jiae.v1i2.22

Network Security Monitoring System Via Notification Alert

Rachmat Muwardi[1], Hongmin Gao[2], Harun Usman Ghifarsyam[3], Mirna Yunita[4], Andika Arrizki[5], Julpri Andika[1]

[1] 1Department of Electrical Engineering, Faculty of Engineering, Universitas Mercu Buana, Indonesia
[2]School of Information and Electronics, Beijing Institute of Technology, China
[3]School of Computer and Information Technology, Beijing Jiaotong University, China
[4]School of Computer Science and Technology, Beijing Institute of Technology, China
[5]IP Specialist, PT. Nokia Solution Networks, Indonesia

Abstract

The development of information technology nowadays has become faster, and this makes network security become important. A huge increasing number of computers that are connected makes many gaps in a network. An administrator has an important role in protecting the security of the network. The problem comes when an administrator has human problems such as pain, negligence, and tiredness while needing rapid information when there is an intrusion on the network. This problem can be solved by adding a data traffic detection system known as Intrusion Detection System (IDS). IDS will be connected to Mail Gateway until that administrator can receive notifications such as alerts during an intrusion to the network anytime and anywhere. Snort as one of the network security systems should be developed as a security detection system and network security. A security intrusion prevention system or an Intrusion Prevented System (IPS). The author tries to do analysis and testing on the subjects above to produce a system capable of detecting the intruder in a network that is mobile and also makes it easy for administrators to open data anywhere and anytime using any device.

Keywords:
Administrators;
Gateway;
IDS;
Monitoring;
Network;
Snort:

Article History:
Received: November 1, 2021
Revised: November 9, 2021
Accepted: November 10, 2021
Published: November 30, 2021

Corresponding Author:
Rachmat Muwardi
Department of Electrical Engineering, Universitas Mercu Buana, Indonesia
Email:
rachmat.muwardi@mercubuana.ac.id

INTRODUCTION

Early in history, humans exchanged information through language. Language is a technology that allows a person to understand the information conveyed by others, but this does not last forever. Information in the hands of the recipient can be forgotten and cannot be stored for much longer. Apart from that, the sound also has limitations. Another technology that can be used to convey information is through images. Images allow a person to get more information and can be taken home and communicated to others. In addition, there is some information that can last longer. For example, some images of ancient relics still exist today to understand the information conveyed by the maker. The discovery of the alphabet facilitates a more efficient delivery of information. Pictures representing events are created by combining alphabets or writing numbers, such as the MCMXLIII in 1943. This alphabet technology makes information easy.

Then, printing technology allows for faster transmission of information. Electronic technologies such as radio, television, and computers are becoming faster so that information is spread over a wider area and can be stored for longer. The development of information technology, particularly networks and computer service, facilitates daily work. However, on the other hand, some problems must be considered, namely the safety factor that is vulnerable to criminal technology. Today, humans are very dependent on information systems; on the other hand, criminal cases also increase sharply on technology and information.

Once authenticated, the firewall enforces access policies such as what services network users access. While preventing unauthorized access, these components may fail to run malicious content such as computer worms or Trojans transmitted over the network. Anti-virus software or intrusion prevention system (IPS) aids and blocks the action of the malware [1][2]. Anomaly-based intrusion detection systems can also reach networks such as Wireshark traffic and can be identified for later high-level auditing and analysis purposes. Newer systems combining unsupervised machine learning with complete network traffic analysis can lead to active network attackers from malicious insiders or targeted external attackers who have compromised machines or user accounts [3][4]. Then, [5, 6, 7] in research using Snort IDS to create a security system capable of countermeasures because the consequences are very bad for the system. The security system was created based on a website capable of security holes, including back doors. Similar research on IDS Snort was conducted by [8], which resulted in a very good IDS Snort for detecting attacks into the network.

The condition can occur because administrators lack information system security and defence against disruption of activities currently being carried out manually. This results in system integrity depending on the availability and speed of the administrator. In addition, administrators must always be on standby to see network conditions in case of interference. Therefore, an administrator is needed today, especially in companies/institutions implementing computer and Internet technology to support work.

The use of computer network systems on a small and wide scale will require settings from the physical and non-physical levels. Process control arrangements. Effective network administrator and enter all network system resources for more effective network performance and views of the functions, structure, and the network itself. However, the downside is that this can lead to virtual machines vulnerable to cyberattacks, such as Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. The attack can attack and consume resources owned by the server or machine to cause the service to become unavailable [9, 10, 11].

METHOD

Network security begins with authenticating, generally with a username and password. Since this only requires one detail authenticating the username, this password is sometimes called one-factor authentication. With two-factor authentication, something the user also uses (for example, a security token or 'dongle,' ATM card, or cell phone); with three-factor authentication, something the user 'is' is also used (fingerprint or retina scan) [12][13].

An Intrusion Detection System (abbreviated as IDS) is a method that can be used to monitor the activity being examined in a system or network. The first, [14][15], published a study outlining ways to improve computer security auditing and surveillance on customer sites. Furthermore, [16][17] developed the first model of IDS in real-time. This prototype is named the Intrusion Detection Expert System (IDES). IDES was originally a rule-based expert system that checks for known malignancies.

A wide spectrum of IDSs varies from anti-virus software to hierarchical systems that backbone traffic throughout the network. The most common classifications are network intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS). Systems that analyze critical operating system files are examples of HIDS, while systems that analyze incoming network traffic are examples of NIDS. It is also possible to classify IDS with a detection approach: the most well-known variants are signature-based detection (exception of bad patterns, such as malware) and anomaly-based detection (monitoring of deviations from the "good" traffic model, which often relies on machine learning). Some IDSs can detect detected intrusions. Systems with responsiveness are commonly referred to as intrusion prevention systems.

It also explained that computer network security is an essential factor that must be tried. Guaranteed security can avoid losses caused by attacks on network security systems. The most common prevention against network attacks is to put the administrator. The problem will arise when the administrator is not a network for this problem, [18][19] in his research using IDS to see activity on the network through automation of administrator work functions. From the research results, administrators can see intrusions that occur on computer networks. The presence of instant messaging applications can help administrators get real-time notifications, one of which is by using the Telegram application. Based on the results of his research, Snort can carry out attacks on computer networks, and the system can send real-time alerts from Snort to administrators via telegram bots. This can be a reference for the use of Snort. Snort is a detection sensor for network treatment errors, this system functions as a grunt NIDS (Network Intrusion Detection System), which controls any intrusion attempts (intrusion).

Then also, the research conducted by [20] also applied the IDS method to problems in cybercafes to overcome the problem of network security that is less than optimal. Several problems were found in the absence of a security system for the cafe servers. Therefore, several times, the cafe servers experienced problems due to attacks carried out by other parties such as ping floods, smurf attacks, and others. Similarly, [21] uses the Intrusion Detection System (IDS) approach as a network activity approach. With this method, IDS provides information for the maintenance of officers who have been given rules.

Threat detection is a priority security solution that must be integrated even in the primary security platform. An intrusion Detection System (IDS) is a device or software application that networks or systems for malicious activity or policy. Any activity or collection is known to be reported by administrators or collected centrally using a security information and event management system (SIEM). The SIEM system combines outputs from multiple sources and uses alarm filtering techniques to distinguish dangerous activity from false alarms [22, 23, 24].

Another research was conducted by [25, 26, 27], who implemented IDS in Senior High School network systems. This waiting system will be implemented using the Intrusion Detection System (IDS) application, namely Snort and PfSense (Router OS), to follow the generated alerts. Based on attempted attacks with a computer with a snort attached, you can see what is happening, resulting in alerts such as the Ping of Death attack and a Port Scan. In addition, PfSense displays a warning if someone tries to abuse the network, such as accessing social media, Facebook, YouTube, Twitter, etc. You can follow up by blocking it automatically.

Then the last one, [28], built a snort system using IDS in his research. They produce intrusion detection systems as an efficient network security tool for traffic work. They generate association alerts after abnormal behavior patterns are adjusted to a set of rules.

Material

The material supports research in designing and implementing system applications "network security monitoring system via notification."

Understanding Intruders

An intruder is a person who performs actions that are distorted, inaccurate, and inappropriate.

Basic Concept of Networking Security

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which the network administrator controls. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs, conducting transactions and communications among businesses, government agencies, and individuals. Networks can be private, such as within a company, and others open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network and protects and overseas operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

IDS (Intrusion Detection System)

The Intrusion Detection System (IDS) is a device or software application that monitors a network or system for malicious activity or policy violations. Any detected activity or violation is typically reported to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources and uses alarm filtering techniques to distinguish malicious activity from false alarms.

There is a wide spectrum of IDS, varying from anti-virus software to hierarchical systems that monitor the traffic of an entire backbone network. The most common classifications are network intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS). A system that monitors important operating system files is an example of a HIDS, while a system that analyzes incoming network traffic is an example of a NIDS. It is also possible to classify IDS by detection approach: the most well-known variants are signature-based detection (recognizing bad patterns, such as malware) and anomaly-based detection (detecting deviations from a model of “good” traffic, which often relies on machine learning). Some IDS can respond to detected intrusions. Systems with response capabilities are typically referred to as intrusion prevention systems.

Server

A server is a computer program or a device that provides functionality for other programs or devices, called “clients.” This architecture is called the client-server model, and a single overall computation is distributed across multiple processes or devices. Servers can provide various functionalities, often called “services,” such as sharing data or resources among multiple clients or performing computation for a client. A single server can serve multiple clients, and a single client can use multiple servers. A client process may run on the same device or connect over a network to a server on a different device. Typical servers are database servers, file servers, mail servers, print servers, web servers, game servers, and application servers.

Client

A client is a piece of computer hardware or software that accesses a service made available by a server. The server is often (but not always) on another computer system, in which case the client accesses the service by way of a network. The term applies to the role that programs or devices play in the client-server model.

Threat

A threat is a communicated intent to inflict harm or loss on another person. A threat is considered an act of coercion. Threats (intimidation) are widely observed in animal behavior, particularly in a ritualized form, chiefly to avoid unnecessary physical violence that can lead to physical damage or the death of both conflicting parties.

Some of the more common types of threats forbidden by law are those made with an intent to obtain a monetary advantage or to compel a person to act against his or her will. In all US states, it is an offence to threaten to use a deadly weapon on another person, injure another's person or property, or injure another's reputation.

Method

The design flowchart of this research can be seen in Figure 1. In running Server, we use laptops with Intel Core I7-7700U CPU @ 2.80GHz (8 CPUs) with 16 GB RAM with Ubuntu operating system to run a Web Server and IDS Snort. The system design uses Snort as IDS for network security. The researcher used the Ubuntu server system operation, which was like all servers in general. Figure 2 shows the block diagram of the system design.

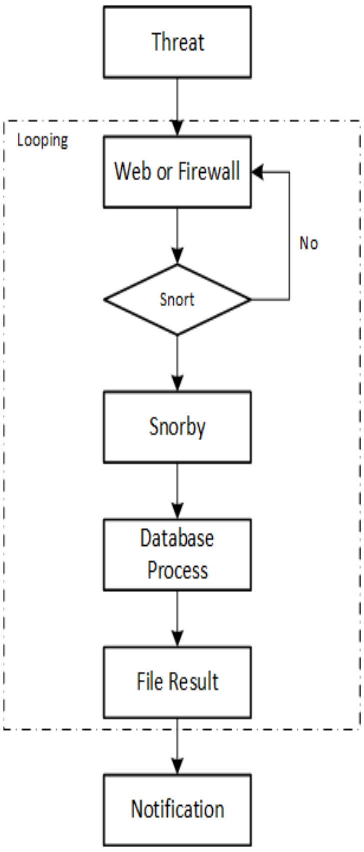

Figure 1. Research Flowchart

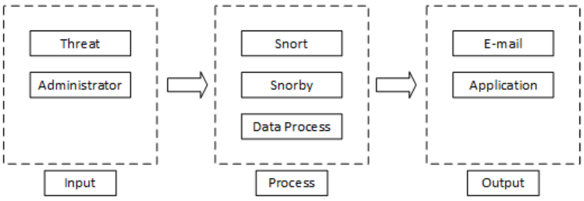

Figure 2. Block Diagram

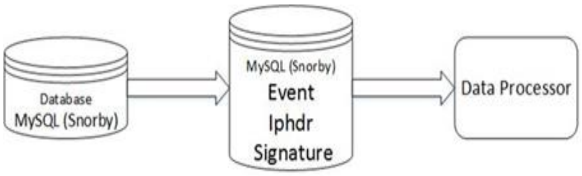

Figure 3. The Process of Retrieving Data

In a network security monitoring system, monitoring and results can be obtained by connecting the MySQL database. They are retrieving data from MySQL Snorby (Event, Iphdr, Signature) using the Data Processor. In other words, this tool is useful for notifying all attacks such as pinging the server or login administrator access somewhere other than the server. In Figure 3, the work steps will be carried out. From this data, all notification data will be sent in the form of a .txt file where the file is in the form of writing containing the type of attack, day, date, and level of the attack.

The actor is the Threat. Then obtained a use case diagram and some scenarios that show interactions use case diagram with actors in the use case diagram. Figure 4 shows the Application Use Case diagram.

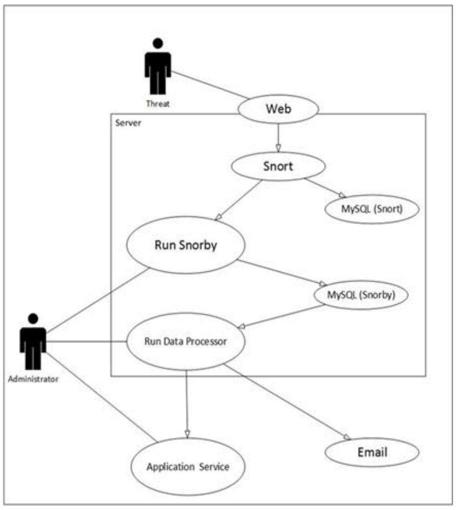

Figure 4. Application Use Case

Below will explain Figure 1 and Figure 2 how it will be processed.

1) Snorby. Network security monitoring interacting with Snort System analysis of threats Ready to Start Generates raw reports based on SNORBY table format. When the administrator run the snorby. How to run snorby by using the terminal. sudo/var/www/html/snorby/. sudo bundle exec rails server-e production Then the system will start to snorby on port 3000.

2) Snort open-source network intrusion prevention system (NIPS) and network intrusion detection system (NIDS) Packet logging on Internet Protocol and Perform real-time traffic analysis Initialized by boot up Generates raw reports based on SNORBY table format. Snort at work when the threats came. Works by using signature detection, functioning also as a sniffer and packet logger. Then snort send threat data to MySQL snort by using barnyard. The last step snort sends threat data to snorby
3) Data Processor. Process data from snorby to desired destination Move data from MySQL snorby to the destination folder, Change MySQL data to file .txt, Translate data for MySQL to file .txt, make file indeks and send an email when there is a threat of priority 1. Started by infinite-loop to generate data priority 1.2 and 3 in the form of a txt file and send data directly to the email's priority 1.
4) Email Alert. Get Threat of warning from the server Notification of warning from the server and Notification type of Threat and level from the server. Initialized by the shell command from the data processor email sent. The Mail Alert will work when the Data processor is getting results and sent using the mail service. Then sent data and received three data, namely high, medium, and low. high data received in 1 minute, medium received in 1 hour, and low received in 1 day
5) Application Service (Client). Get Threat Data to form the Server Notification of warning from the server and Notification type of Threat and level from the server. The user-generating report initializes them. It will work when the data processor gets results, and the Application Service can get data using the FTP protocol.

RESULTS AND DISCUSSION

This section contains the test results and the implementation of the Network Security Monitoring System via Notification Alert. This test consists of Threat, Server, and Client.

Implementation System

After the system is analyzed and designed in detail, the next step is implementation. System implementation is the stage of putting the system so that it is ready for operation. In addition, the implementation aims to confirm the module design so that users can provide input for system development.

IDS Implementation

IDS, or institutional editing system, uses several main components: Snort, Barnyard, and Snorby. The IDS built on the Ubuntu server follows several processes that are carried out before deploying. The meaning of the apt-get install command, according to Table 1, is the command to install new packages. All packages are installed in the root because the root is the highest user status in the operating system, meaning that all file systems, documents, and anything can be accessed by root install Snort.

Table 1. Install Packet Support IDS

No.	Install Packet Support IDS
1	apt-get update
2	apt-get dist-upgrade
3	Apt-get install mysql -common -client -server
4	Apt-get install php -dev -idap -mysql -pear

System Test

The testing process is done by installing an application on the device. In this case, I will use the Blackbox application testing method. To see whether the function of the application is running well or not and to find out if there are errors in this application to be immediately fixed by the maker. Consists of Threat, Server, and Client contained in the "Network Security Monitoring System via Notification Alert" As seen below, the researcher desired the results.

In Table 2, Threat Test Results that threat testing gets the expected results. There is no problem with this test even though it is repeated continuously. In Table 3, Server Test Results that the Snort and Snorby tests got the expected results.

Table 2. Threat Test Result

No	Name of Testing	Nature of Activity	Expected Result	Test Result
1	Attack ping	Normal	ICMP traffic	Correct
2	Nmap port scanning attack	Normal	Port Scanning	Correct
3	Digital Blaster	Normal	Port Scanning	Correct

Table 3. Server Test Result

No.	Name of Testing	Nature of Activity	Expected Result	Test Result
1	Snort	Normal	Detection threat	Correct
2	Snorby	Normal	Make priority	Correct
		Normal	Data Rules	Correct
3	Data Processor	Normal	Make txt file priority result	Correct
		Normal	Checkpoint last entry	Correct
		Normal	Get data for MySQL Snorby	Correct
		Normal	Translate Data MySQL (Ipsrc, Ipdst, Signature, Timestamp)	Correct
		Normal	Send Priority High One Minute	Correct
		Normal	Send Priority Medium One Hour	Correct
		Normal	Send Priority Low One Day	Correct

The program can also be used to detect probes or attacks, including, but not limited to, operating system fingerprinting attempts, a common gateway interface, buffer overflows, server message block probes, and stealth port scans.

Snort can be configured in three main modes: sniffer, packet logger, and network intrusion detection. In sniffer mode, the program will read network packets and display them on the console. In packet logger mode, the program will log packets to the disk. In intrusion detection mode, the program will monitor network traffic and analyze it against a rule set defined by the user. The program will then perform a specific action based on what has been identified. Table 4 lists the Client Test Result.

Table 4. Client Test Result

No	Name of Testing	Nature of Activity	Expected Result	Test Result
1	Application Service	Normal	Get data from server	Correct
2	Mail Alert	Normal	Receiver priority high	Correct
		Normal	Receiver priority medium	Correct
		Normal	Receiver priority low	Correct

Discussion

The Mail Alert will work when the Data Processor is getting results and sent using mail service. Then send data. Then received three data, namely high, medium, and low. High data received in 1 minute, medium received in 1 hour, and low received in 1 day. The Application

Service (Client) will work when the Data Processor results, and the Application Service can get data using the FTP protocol.

After carrying out various processes in the IDS application, the authors find it easy to implement. It can be obtained from this IDS application. A computer network can be monitored only through a computer that acts as a sensor in the network and connected to a network, can see all the events that occur in it.

In addition to the benefits obtained in the IDS application, the IDS system also secures the network, namely if this IDS uses snort, where did the attack come from, through some ports, and what protocol was used.

CONCLUSION

Information can quickly get to the administrator via warning notices, so administrators do not have to always be in front of their computer to monitor the network. Attacks can be detected or not depending on the attack pattern is in the Intrusion Detection System rule or not. Intrusion Detection System Manager This system has been able to detect various attacks effort, either in Port scanning, Denial of Service, or Exploit. Snort as one of the network security systems should be developed as a security detection system and network security. A security intrusion prevention system or an Intrusion Prevented System (IPS). Additional modules that support the Intrusion Detection System's performance will help the system work efficiently, such as rule-rule setting and addition of frond endThe conclusion is a summary of the results and discussion and should be written in paragraphs instead of numbering. Moreover, the prospect of developing research results and application prospects of further studies can also be added to the next (based on result and discussion).

ACKNOWLEDGMENT

The first special thanks go to Mercu Buana University for supporting foreign collaborative research, the second to Beijing Institute of Technology, Mirna Yunita, and Prof. Gao Hongmin for their help and cooperation during this research. Third, to Beijing Jiaotong University, Harun Usman Ghifarsyam, for providing unfailing support and continuous encouragement. The last thank goes to the IT team of certain companies. Hopefully, there will always be paper collaborations with the Beijing Institute of Technology and Beijing Jiaotong University in future research.

REFERENCES

[1] S. M. Mohammad and S. Lakshmisri, "Security Automation in Information Technology," *International Journal of Creative Research Thoughts (IJCRT),* vol. 6, no. 2, pp. 901-905, 2018, doi: 10.1729/Journal.24048

[2] P. Clay, "A modern threat response framework," *Network Security,* vol. 4, pp. 5-10, 2015, doi: 10.1016/S1353-4858(15)30026-X

[3] S. N. Narayanan, A. Ganesan, K. Joshi, T. Oates, A. Joshi and T. Finin, "Early Detection of Cybersecurity Threats Using Collaborative Cognition," *2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)*, 2018, pp. 354-363, doi: 10.1109/CIC.2018.00054.

[4] S. Malik, "Cybersecurity: Security Automation and Continous Monitoring," *Doctoral Dissertation*, Utica College, 2018.

[5] G. Krishna, T. Samrat, S. R. Kiran and A. Srisaila, "Testing performance of RaspberryPi as IDS using SNORT," in *Materials Today: Proceedings*, 2021, doi: 10.1016/j.matpr.2021.01.607

[6] S. Badotra and S. N. Panda, "SNORT based early DDoS detection system using Opendaylight and open networking operating system in software defined networking," *Cluster Computing,* vol. 24, no. 1, pp. 501-513, 2021, doi: 10.1007/s10586-020-03133-y

[7] A. I. A. Suwailem, M. Al-Akhras and K. K. A. Ghany, "Evaluating Snort Alerts as a Classification Features Set," in *Applications of Artificial Intelligence in Engineering. Springer*, Singapore, 2021.

[8] S. Sasikumar, “Network Intrusion Detection and Deduce System,” *Turkish Journal of Computer and Mathematics Education (TURCOMAT),* vol. 12, no. 9, pp. 404-410, 2021, doi: 10.17762/turcomat.v12i9.3094

[9] D. Fadhilah and M. I. Marzuki, “Performance Analysis of IDS Snort and IDS Suricata with Many-Core Processor in Virtual Machines Against Dos/DDoS Attacks,” *2020 2nd International Conference on Broadband Communications, Wireless Sensors and Powering (BCWSP)*, 2020, pp. 157-162, doi: 10.1109/BCWSP50066.2020.9249449.

[10] M. Jonker, A. King, J. Krupp, C. Rossow, A. Sperotto and A. Dainotti, “Millions of targets under attack: a macroscopic characterization of the DoS ecosystem,” in *In Proceedings of the 2017 Internet Measurement Conference*, 2017, pp. 100-113, doi: 10.1145/3131365.3131383

[11] S. Velliangiri, P. Karthikeyan and V. V. Kumar, “Detection of distributed denial of service attack in cloud computing using the optimization-based deep networks,” *Journal of Experimental & Theoretical Artificial Intelligence,* vol. 33, no. 3, pp. 405-424, 2021, doi: 10.1080/0952813X.2020.1744196

[12] F. Sadikoglu and S. Uzelaltinbulat, “Biometric retina identification based on neural network,” in *Procedia Computer Science*, vol. 102, pp. 26-33, 2016, doi: 10.1016/j.procs.2016.09.365

[13] N. Uddin, S. Zia, F. Shamail, F. Zia and S. J. Ali, “Adermatoglyphia (Loss of Fingerprints) in Young Female Patient Having the Conditions of Hyperhidrosis and Atopic Dermatitis,” *Liaquat National Journal of Primary Care ,* vol. 3, no. 1, pp. 39-40, 2021, doi: 10.37184/lnjpc.2707-3521.3.10

[14] J. P. Anderson, “Computer security threat monitoring and surveillance,” *Technical Report*, James P. Anderson Company, 1980.

[15] T. F. Stafford, “Platform-Dependent Computer Security Complacency: The Unrecognized Insider Threat,” in *IEEE Transactions on Engineering Management*, pp. 1-12, 2021, doi: 10.1109/TEM.2021.3058344.

[16] D. Denning and P. G. Neumann, *Requirements and model for IDES-a real-time intrusion-detection expert system*, Menlo Park: SRI International, 1985.

[17] S. Gavel, A. S. Raghuvanshi and S. Tiwari, “Maximum correlation based mutual information scheme for intrusion detection in the data networks,” *Expert Systems with Applications,* vol. 189, 116089, 2021, doi: 10.1016/j.eswa.2021.116089

[18] A. Erlansari, F. F. Coastera and A. Husamudin, “Early Intrusion Detection System (IDS) using Snort and Telegram approach,” *SISFORMA ,* vol. 7, no. 1, pp. 21-27, 2020.

[19] R. G. M. Ibrahim, “Performance Assessment of Snort-based Network Intrusion Detection System,” *Doctoral Dissertation*, Sudan University of Science and Technology, 2021.

[20] S. Sarika, S. Velliangiri and M. Ravi, “A detection of IoT based IDS attacks using deep neural network,” in *AIP Conference Proceedings*, vol. 2358, 130001, 2021, doi: 10.1063/5.0057952

[21] E. Nasri, R. Kania and S. Tsauri, “Network Integration and Security Using IDS and Tunneling Methods,” in *1st International Multidisciplinary Conference on Education, Technology, and Engineering (IMCETE 2019)*, 2020, doi: 10.2991/assehr.k.200303.023

[22] E. Alaoui and Y. Gahi, “Network Security Strategies in Big Data Context,” in *Procedia Computer Science*, vol. 175, pp. 730-736, 2020, doi: 10.1016/j.procs.2020.07.108

[23] A. Firdausi, L. Damayanti, G. P. N. Hakim, U. Umaisaroh, and M. Alaydrus, “Design of A Dual-Band Microstrip Antenna for 5G Communication,” vol. 1, no. 1, pp. 65-72, 2021, doi: 10.51662/jiae.v1i1.15

[24] S. A. Fadhil, “Internet of Things security threats and key technologies,” *Journal of Discrete Mathematical Sciences and Cryptography ,* pp. 1-7, 2021, doi: 10.1080/09720529.2021.1957189

[25] J. Manhas and S. Kotwal, “Implementation of Intrusion Detection System for Internet of Things Using Machine Learning Techniques,” in *Multimedia Security. Springer*, Singapore, 2021.

[26] B. Kerim, “Securing IoT Network against DDoS Attacks using Multi-agent IDS,” in *Journal of Physics: Conference Series*, vol. 1898, no. 1, 012033, 2021, doi: 10.1088/1742-6596/1898/1/012033

[27] R. Babu, “Design, Implementation, and Field-Testing of Distributed Intrusion Detection System for Smart Grid SCADA Network,” *Doctoral Dissertation*, Iowa State University, 2021.

[28] N. Khamphakdee, N. Benjamas and S. Saiyod, “Improving Intrusion Detection System Based on Snort Rules for Network Probe Attacks Detection with Association Rules Technique of Data Mining,” *Journal of ICT Research & Applications,* vol. 8, no. 3, 2015, doi: 10.5614/itbj.ict.res.appl.2015.8.3.4