Accredited Ranking SINTA 2
Decree of the Director General of Higher Education, Research and Technology, No. 158/E/KPT/2021
Validity period from Volume 5 Number 2 of 2021 to Volume 10 Number 1 of 2026

Published online on: **http://jurnal.iaii.or.id**

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 7 No. 5 (2023) 1132 - 1139 ISSN Media Electronic: 2580-0760

Network Attacks Classification for Network Forensics Investigation: Literature Reviews

Muhamad Maulana[1], Ahmad Luthfi[2], Dwi Kurnia Wibowo[3]
[1,2,3]Department of Informatics, Faculty of Industrial Technology, Indonesian Islamic University, Yogyakarta, Indonesia
[1]vanmoeljr8@gmail.com, [2]ahmad.luthfi@uii.ac.id, [3]dwikurniawibowo@gmail.com

Abstract

Every branch of technology must constantly be on guard and anticipate the possibility of numerous cybercrimes due to the ongoing cyber-attacks. Crimes committed in this era of digitalization will undoubtedly have a negative impact on individuals or groups. In order to allow any cybercriminal to operate freely without worrying about getting caught, mitigation after a cyber-attack is often considered a trivial problem. Digital forensics not only plays an important role in the digitization cycle but is also critical to the digital industry's ability to respond to events as they occur. The standard methods used to support the pace of progress in digital forensics are very time-consuming and ineffective given the frequency of cybercrime. It is expected that collaboration between technology disciplines, such as the application of machine learning to digital forensics, will improve the efficiency of the forensic analysis and investigation process. These recommendations propose the application of machine learning techniques for automated attack classification using network logs. Specifically, machine learning algorithms would be trained to detect DDoS, SQL Injection, and XSS attacks based on the traffic logs on the router. The chosen method for this classification task is Support Vector Machine (SVM), which has been extensively employed in data-driven classification tasks according to previous research. By leveraging machine learning, the goal is to streamline the investigation of computer network attacks, making it faster and more efficient.

Keywords: network attacks; classification; machine learning; investigation

1. Introduction

The internet is now widely used by most individuals for a variety of professional and personal tasks due to rapid technological advancements that make it easily accessible. The Internet is used for several important activities, including communication, information exchange, and economic transactions. The Internet promotes connection and communication, but attackers aiming to damage and disrupt network connections and network security can violate and jeopardize the integrity and confidentiality of connections and information exchange [1]–[5].

Network attacks are becoming more frequent over time, requiring their investigation, understanding, and development as more effective security defense technologies. Network security solutions are required for every business, sector, and level of government to protect against the increasing threat of cyberattacks. As no network is immune to network attacks, the need for more reliable and effective network security systems to protect customer and business data is increasing.

Network forensics is the collection, recording, and investigation of network events with the goal of identifying the origin of security attacks or other instances of problems. In other words, network forensics entails the collection, cataloging, and examination of network traffic. Network forensics serves to gather information, compile evidence, and identify attacks. When managing activity and traffic on the network, investigative procedures are performed. Unlike other means, network forensics deals with dynamic information that tends to be lost. The network forensics investigation process used consists of several stages consisting of nine stages referred to as the Generic Framework for Network Forensics[6]–[10].

According to a Kaspersky report, DDoS attacks are frequent and hostile every quarter, with a wide range of subjects, including politics, education, business, and others [11], [12]. Amazon in February 2020, NetScout in April 2018, and GitHub in February 2018 are just a few examples of industries where the most frequent DDoS attacks have occurred [13]–[15]. As seen in Figure 1 from Cisco's Annual Internet Report 2018-2023, DDoS attacks continue to increase year over year,

Accepted: 09-06-2023 | Received in revised: 16-09-2023 | Published: 01-10-2023

making it difficult to prevent the scale of DDoS attacks that are still occurring today, according to Kaspersky. Maintaining service resource operations, reviewing Internet service provider contracts, implementing specialized solutions such as DDoS protection, understanding network traffic, and establishing a backup defense strategy are all ways to reduce DDoS attacks.

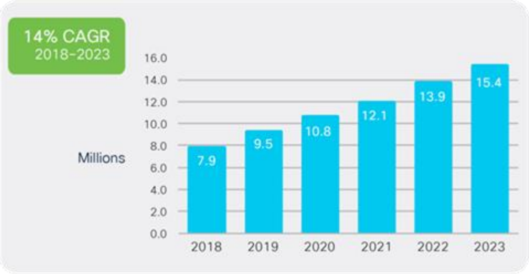

Figure 1. Cisco DDoS Annual Report

Still common and unpredictable, injection attacks are a component of cyber-attacks. From a few years ago to the present, several cyber events have taken place. The discovery of SQL injection vulnerabilities in Cisco Prime License Manager in 2018, SQL injection in the video game Fortnite in 2019, and SQL injection attacks on the Estonian Central Health Database in 2020, which allowed the perpetrators to access the medical records of almost all Estonian citizens, are just a few of the incidents that have occurred in recent years [16], [17]. Attempts can be made to reduce SQL injection attacks by ensuring that the system in use is updated in every way, staying abreast of the risks, and developing strategies to anticipate them.

This paper aims to explore the latest research on attacks on computer networks. Attacks on computer networks that vary greatly are then classified and mapped. The process of classifying and mapping attacks on computer networks is proposed for future research.

2. Research Methods

This literature reviews collected literature studies related to attacks on computer networks as seen in Figure 2. The search process was conducted using several popular databases, such as Google Scholar and ResearchGate. Google Scholar and ResearchGate were chosen because they can find a wide range of journals and are suitable for searching in very specific research domains. The search was conducted using important keywords, such as "network attack", "network hacking", "network forensics", and "machine learning".

Collection and analysis were conducted from January to April 2023. The selection process was based on the title, abstract, purpose, and type of network attack. Scientific papers that met the selection criteria were included in the literature review. After the selection process, thirty scientific papers were included in the literature review with the theme of attacks that occur on computer networks.

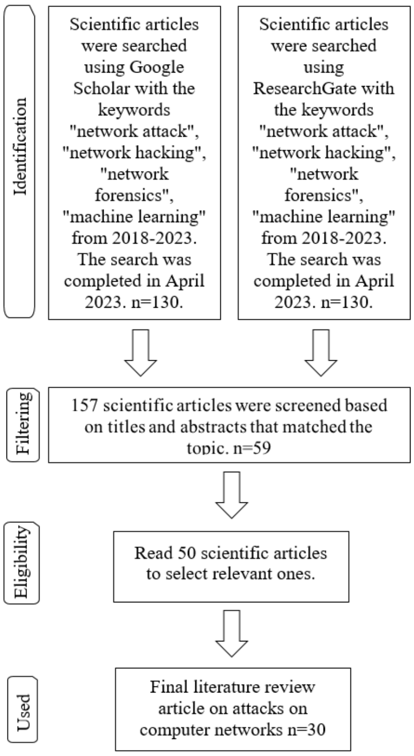
Identification
Scientific articles were searched using Google Scholar with the keywords "network attack", "network hacking", "network forensics", "machine learning" from 2018-2023. The search was completed in April 2023. n=130.
Scientific articles were searched using ResearchGate with the keywords "network attack", "network hacking", "network forensics", "machine learning" from 2018-2023. The search was completed in April 2023. n=130.
Filtering
157 scientific articles were screened based on titles and abstracts that matched the topic. n=59
Eligibility
Read 50 scientific articles to select relevant ones.
Used
Final literature review article on attacks on computer networks n=30

Figure 2. Flowchart of the literature review of attacks on computer networks.

3. Results and Discussions

The results of the search conducted are mapped in Table 1 and Table 2, the mapping carried out then results in the conclusion of attack categories that often occur based on vulnerabilities in the service system. The categories of attacks that occur include DDoS, Injection, Hijacking.

Broken Access Control vulnerabilities are often used to attack from the network side. The attack is in the form of flooding access requests so that the system cannot serve users. This attack is called DDoS, in Figure 3, 4, 5 describes the types of DDoS [18]–[20].

Software and Data Integrity Failures vulnerabilities are also often exploited by attackers from the network side. This attack is more focused on the source code of the application system that is hijacked and manipulated. This is very dangerous because it has an impact on changing the function of the application system. This source code manipulation by attackers is often called Cross Site Scripting (XSS). The XSS mechanism is described in Figure 6 [21]. Identification and Authentication Failures vulnerabilities are also widely utilized by attackers to carry out attacks from the network side. This attack is more focused on the data repository of a system or database. This attack is carried out by injecting payload code to illegally access the

DOI: https://doi.org/10.29207/resti.v7i5.5153

database. The attack mechanism is called SQL Injection, described in Figure 7 [7], [22].

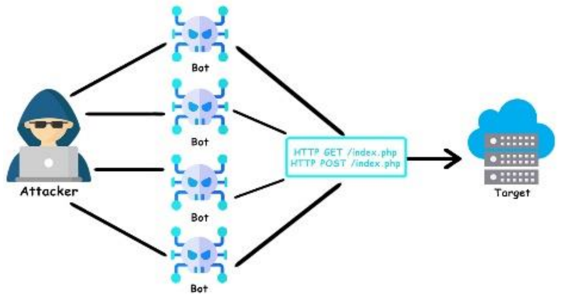

Figure 3. DDoS Application Attack

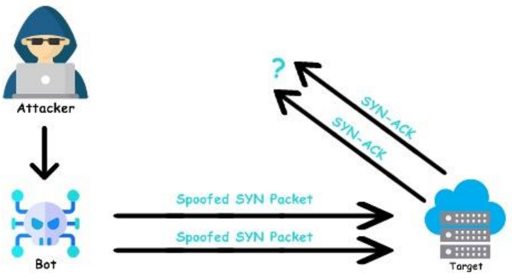

Figure 4. DDoS Protocol Attack

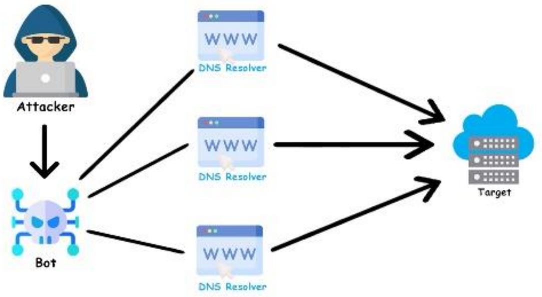

Figure 5. DDoS Volumetric Attack

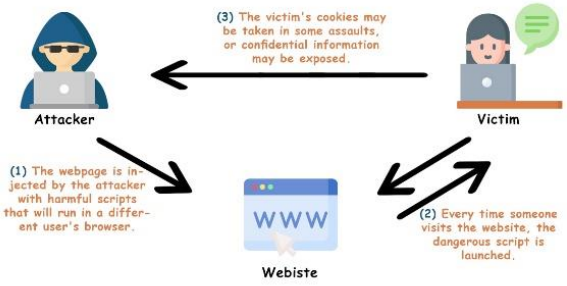
(3) The victim's cookies may be taken in some assaults, or confidential information may be exposed.
Attacker
Victim
(1) The webpage is in-jected by the attacker with harmful scripts that will run in a differ-ent user's browser.
WWW
Webiste
(2) Every time someone visits the website, the dangerous script is launched.

Figure 6. XSS Attack

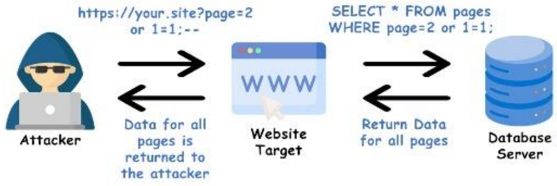
https://your.site?page=2 or 1=1;--
SELECT * FROM pages WHERE page=2 or 1=1;
Attacker
Data for all pages is returned to the attacker
WWW
Website Target
Return Data for all pages
Database Server

Figure 7. SQL Injection Attack

The literature reviews conducted in Table 1 and Table 2 is the result of mapping previous research related to attacks on computer networks. The studies taken are those that discuss vulnerabilities related to Broken Access Control, Software and Data Integrity Failures, and Identification and Authentication Failures.

Attack mechanisms based on the vulnerabilities mentioned include DDoS, Hijacking and Injection. The results of the search conducted are mapped in Table 1 and Table 2, the mapping carried out then results in the conclusion of attack categories that often occur based on vulnerabilities in the service system. The categories of attacks that occur include DDoS, Injection, Hijacking.

Table 1. Summary of Literature Reviews

Attack	Literature	Vulnerability	Attack Type	Objective
2018	[23]	Broken Access Control	DoS, DDoS	Flooding network traffic
2018	[24]	Broken Access Control, Software and Data Integrity Failures	DoS, Injection	Flooding network traffic, inserting content not in line with service functions
2018	[25]	Broken Access Control	DDoS	Flooding network traffic
2018	[26]	Broken Access Control	DDoS	Flooding network traffic
2018	[27]	Broken Access Control	DoS	Flooding network traffic
2018	[28]	Broken Access Control	DDoS	Flooding network traffic
2018	[29]	Software and Data Integrity Failures	Injection	Inserting content does not match the service function
2018	[20]	Broken Access Control	DDoS	Flooding network traffic
2018	[30]	Broken Access Control	DoS	Flooding network traffic
2018	[31]	Software and Data Integrity Failures	Injection	Inserting content does not match the service function
2019	[32]	Software and Data Integrity Failures	Injection	Inserting content does not match the service function
2019	[33]	Software and Data Integrity Failures	Injection	Inserting content does not match the service function
2019	[21]	Software and Data Integrity Failures	Injection	Inserting content not in accordance with the service function

DOI: https://doi.org/10.29207/resti.v7i5.5153

Table 2. Summary of Literature Reviews (Continued)

Attack	Literature	Vulnerability	Attack Type	Objective
2019	[2]	Identification and Authentication Failures	Hijacking	Manipulating packets
2020	[18]	Broken Access Control	DDoS	Flooding network traffic
2020	[34]	Broken Access Control, Software and Data Integrity Failures, Identification and Authentication Failures	DoS, Injection, Hijacking	Flooding network traffic, inserting content that does not match the service function, manipulating packets
2020	[35]	Software and Data Integrity Failures	Injection	Inserting content not according to service function
2020	[36]	Identification and Authentication Failures	Hijacking	Manipulate packets
2020	[37]	Identification and Authentication Failures	Hijacking	Manipulate packets
2020	[38]	Identification and Authentication Failures	Hijacking	Manipulate packets
2021	[19]	Broken Access Control	DDoS	Flooding network traffic
2021	[6]	Software and Data Integrity Failures	Injection	Inserting content that does not match the service function
2021	[22]	Software and Data Integrity Failures	Injection	Inserting content that does not match the service function
2021	[39]	Software and Data Integrity Failures	Injection	Inserting content that does not match the service function
2021	[40]	Broken Access Control, Identification and Authentication Failures	DoS, Hijacking	Flooding network traffic, manipulating packets
2022	[41]	Broken Access Control	DDoS	Flooding network traffic
2022	[42]	Software and Data Integrity Failures, Identification and Authentication Failures	Injection, Hijacking	Inserting content not according to service function, manipulating packets
2022	[43]	Broken Access Control, Software and Data Integrity Failures, Identification and Authentication Failures	DDoS, Injection, Hijacking	Flooding network traffic, inserting content not according to service function, manipulating packets
2022	[44]	Broken Access Control	DDoS	Flooding network traffic
2023	[45]	Identification and Authentication Failures	Hijacking	Manipulate packets

The rapid development of the internet has forced most business organizations to follow the current trend by coming up with modern and flexible technological innovations and developments for business processes. DDoS attacks are not the only cyber-attacks that have a significant and detrimental impact. OWASP as a cybersecurity observer organization categorizes cyber-attacks into several categories so that a Top 10 attack is made that informs the type of vulnerability and the impact of threats that occur on a device, so that this information can be used either by individuals or organizations to make decisions in evaluating security risks on devices that are managed [46].

Several methods have been proposed to handle and categorize network traffic attacks. First is the port-based approach, which entails selecting port numbers from those kept on file by the Internet Assign Number Authority (IANA). However, this method has proven ineffective due to the increasing number of applications and unreliable ports. In addition, this method is not applicable to applications that use dynamic port numbers or account applications that do not register their ports with IANA. Another method that has been suggested is the payload-based method, commonly known as Deep Packet Inspection (DPI), where the contents of network packets are examined and compared with a data set on a database. This method provides more accurate results than port-based techniques but does not work on network applications that use encrypted data [47]–[49].

DDoS attacks, which can prohibit authorized users from accessing network services, are one of the most frequent and dangerous forms of attacks. Servers can become the target of DDoS attacks by flooding the network with huge volumes of traffic, which can exhaust network resources. In addition, there are many devices that can connect to the Internet due to the IoT era. As a result, attackers can use many bots from different places to launch various DDoS attacks. It is difficult to identify DDoS attacks carried out using bot devices [18]–[20].

In addition, these attacks quickly exhaust network resources. A significant DDoS attack can cost some businesses up to $100,000 per hour while also eroding client trust. DDoS attacks can overload multiple levels of SDN, including the channels for communication between the controller and the application layer or between the controller and the open flow switch. SDN has a single point of failure, so if it is destroyed by a DDoS attack, the entire network will go down at once [6], [32], [33], [41], [43].

Substantial recovery costs are an additional loss for agencies due to the loss of integrity caused by cyber-attacks that have occurred. Activities that damage,

DOI: https://doi.org/10.29207/resti.v7i5.5153

disrupt, steal data, and anything that harms system owners on computer networks are illegal and can be prosecuted in court. Criminals can be punished based on evidence found by network forensics mechanisms [6], [19], [23], [33], [42].

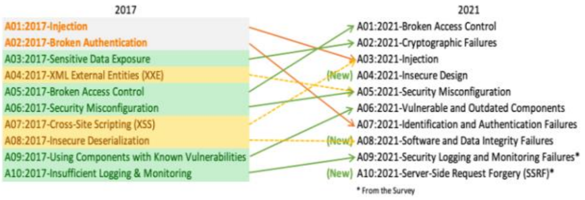
2017
A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring
2021
A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
(New) A10:2021-Server-Side Request Forgery (SSRF)*
* From the Survey

Figure 8. *OWASP Top 10 differences 2017 vs 2021*

Investigators commonly use network monitoring systems such as IDS for forensic purposes, where investigations are conducted using IDS logs and attack notification systems. Intrusion Detection System (IDS) works by monitoring and alerting suspicious activities that occur on the network and immediately reporting them as alerts. Most of the time, intrusion detection systems are used based on digital signatures. Due to the variation in network traffic, which results in a growing number of alerts because the data flow in the network is not stationary to generate and respond to alerts, this results in many errors in detecting attacks. Network traffic can also be viewed by analyzing network packets. Network packets are a fundamental object that can be analyzed in network forensics, this is done to collect data related to network traffic that can be used as evidence in court [21], [34], [39], [44].

Structured Query Language (SQL) Injection and Cross Site Scripting (XSS) attacks are one of the top 10 types of attack categories according to OWASP, but in the OWASP TOP 10 Web Application Security Risk 2021 there are several category changes and there are new categories. The update categorizes XSS attacks as part of the injection attack category. Unlike DDoS attacks that occur at layer 3 network and layer 4 transport, injection attacks in the Open Systems Interconnection model (OSI model) can occur at layer 5 session, layer 6 presentation and layer 7 application. Figure 8 explains the difference in OWASP's top attack categories in 2017 and 2021.

The main threats of injection attacks include theft of credentials, forced access to a system and violation of the integrity of stored data. The number of criminal acts in the cyber world, injection attacks are one form of attack that has a wide range of vulnerabilities, including SQL Injection, Command Injection, XSS, NoSQL Injection, LDAP Injection, and others. SQL Injection has several basic types In-band SQLi (Classic SQLi), Out-of-band SQLi and Inferential SQLi (Blind SQLi) [31], [50], [51].

The diversity of types and variations of injection attacks makes it one of the critical attacks that can cause major damage to a system, data leakage and can even cause paralysis of the system. The presence of technological innovations and developments at this time still cannot stem the attacks caused by injection vulnerabilities [52]–[54].

SQL Injection attacks perform the injection process on the target database, while XSS attacks inject code with malicious functions that are injected into a system in the form of JavaScript. Some people think that XSS attacks are not a serious threat, but in some incidents XSS attacks have impacted several major services such as PayPal (2006), Amazon (2013) and Twitter (2014). XSS attacks allow the perpetrator to perform various harmful actions including taking over accounts, installing spyware, exploiting the system further, spreading viruses/worms and even remoting the system [55], [56].

XSS attacks work through malicious code that has been inserted into a system that can infect the victim's application system or browser. The code will have various effects depending on what function the XSS code serves. Generally, XSS code is used to steal cookies, read user activity as spyware/keylogger, and spread viruses. These things are often considered not so important, however, such as cookie theft, especially if the stolen cookie is a credential cookie that can be used so that the perpetrator does not need a username/ password to access the victim's data/account [57], [58].

Like SQL Injection, XSS attacks have several types of attacks that have different impacts, namely Reflected XSS, Stored XSS and DOM Based XSS which have different threat levels. The various types of XSS attacks, methods and variants of injection models make this XSS attack a threat that needs to be watched out for, especially since there are still many systems that ignore the threat of this attack, especially in application systems [59], [60].

Machine Learning (ML) and data mining techniques play an important role in cyber-attack detection and classification. Machine learning can be a solution to create mechanisms to detect and identify new types of attacks and help investigators investigate evidence in network forensics. Several machine learning studies have been conducted in various domains of this technique providing anomaly-based intrusion detection functions on network devices. The rapid development of machine learning presents a variety of methods that can be used for various needs with the advantages and disadvantages of these methods. Support Vector Machine (SVM) is one of the machine learning algorithms that can be used in classification due to its ability to clearly classify data points by creating a hyperplane in n-dimensional space, where n represents the number of features [33], [40], [41], [43], [61].

DOI: https://doi.org/10.29207/resti.v7i5.5153

Support Vector Machine (SVM) is a general machine learning model that offers efficient data classification in real-life applications, such as expert systems and anomaly detection. C5 (signature) and one-class SVM (anomaly) classifiers provide superior detection rate results in detection rates and other measurement values in machine learning algorithms. The use of SVM Polynomial algorithm has higher confusion matrix accuracy, precision, recall and f1 score compared to Naïve Bayes algorithm [2], [26], [28], [35], [49], [62].

The use of the Support Vector Machine (SVM) algorithm is considered to have a level of stability in the classification process and has a high accuracy value. The amount of data that appears in the network forensic investigation process is a challenge for an investigator to find evidence related to abnormal network traffic, network communication and files. The presence of machine learning with the implementation of the SVM algorithm is expected to help the network forensic investigation process in finding evidence in the form of abnormal network traffic and evidence of attacks on a system to be more efficient and accurate. The selection of the Support Vector Machine (SVM) algorithm is based on suggestions, recommendations and results from previous studies related to the data classification process using machine learning [32], [35], [48], [49], [62], [63].

4. Conclusion

The literature review conducted in this study reveals a significant variation in the types of attacks perpetrated on computer networks. These attacks can be classified based on the vulnerabilities exploited by the attackers. The contribution of this literature review lies in the classification of network attacks according to their underlying vulnerabilities. Three common vulnerabilities targeted by attackers include Broken Access Control, Software and Data Integrity Failures, and Identification and Authentication Failures. Attackers often exploit these vulnerabilities to carry out attacks such as DDoS, Hijacking, and Injection. Furthermore, this literature review also offers insights into future research recommendations for classifying network attacks using machine learning algorithms. The aim is to automate the attack classification process, thereby expediting investigations. Support Vector Machine (SVM) is a suitable method for this purpose, as it has demonstrated accuracy in data classification in various previous studies.

In addition to the classification of network attacks based on vulnerabilities, future research should focus on developing proactive defense mechanisms to mitigate and prevent such attacks. This can involve the implementation of advanced intrusion detection and prevention systems that leverage machine learning algorithms to identify and respond to emerging threats in real-time. Additionally, exploring the potential of anomaly detection techniques and behavioral analysis can enhance the ability to detect and thwart sophisticated attack patterns. By investing in research and innovation in these areas, organizations can strengthen their network security posture and stay one step ahead of cybercriminals.

References

[1] I. W. Ardiyasa, “Aplikasi Analisis Network Forensic untuk Analisis Serangan pada Syslog Server,” Res. Comput. Inf. Syst. Technol. Manag., vol. 2, no. 2, p. 59, 2019, doi: 10.25273/research.v2i02.5220.

[2] S. Nomm and H. Bahsi, “Unsupervised Anomaly Based Botnet Detection in IoT Networks,” in Proceedings - 17th IEEE International Conference on Machine Learning and Applications, ICMLA 2018, 2019, pp. 1048–1053, doi: 10.1109/ICMLA.2018.00171.

[3] Bita Parga Zen, Anggi Zafia, and Iwan Nofi Yono Putro, “Network Security Analysis Simulation at the GCS in the UCAV to support the Indonesian Defense Area,” J. RESTI (Rekayasa Sist. dan Teknol. Informasi), vol. 6, no. 5, pp. 824–831, 2022, doi: 10.29207/resti.v6i5.4412.

[4] H. Ernita, Y. Ruldeviyani, D. Nurul Maftuhah, and R. Mulyadi, “Strategy to Improve Employee Security Awareness at Information Technology Directorate Bank XYZ,” J. RESTI (Rekayasa Sist. dan Teknol. Informasi), vol. 6, no. 4, pp. 577–584, 2022, doi: 10.29207/resti.v6i4.4170.

[5] F. Yuan, Y. Cao, Y. Shang, Y. Liu, J. Tan, and B. Fang, “Insider threat detection with deep neural network,” Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 10860 LNCS. Springer International Publishing, pp. 43–54, 2018, doi: 10.1007/978-3-319-93698-7_4.

[6] C. Luo, Z. Tan, G. Min, J. Gan, W. Shi, and Z. Tian, “A Novel Web Attack Detection System for Internet of Things via Ensemble Classification,” vol. 17, no. 8, pp. 5810–5818, 2021.

[7] T. P. Latchoumi, M. S. Reddy, and K. Balamurugan, “European Journal of Molecular & Clinical Medicine Applied Machine Learning Predictive Analytics to SQL Injection Attack Detection and Prevention,” vol. 07, no. 02, pp. 3543–3553, 2020.

[8] M. S. Elsayed, N. A. Le-Khac, S. Dev, and A. D. Jurcut, “Machine-Learning Techniques for Detecting Attacks in SDN,” Proc. IEEE 7th Int. Conf. Comput. Sci. Netw. Technol. ICCSNT 2019, pp. 277–281, 2019, doi: 10.1109/ICCSNT47585.2019.8962519.

[9] T. Sianturi and Kalamullah Ramli, “A Security Framework for Secure Host-to-Host Environments,” J. RESTI (Rekayasa Sist. dan Teknol. Informasi), vol. 6, no. 3, pp. 380–386, 2022, doi: 10.29207/resti.v6i3.4018.

[10] R. Adams, V. Hobbs, and G. Mann, “The Advanced Data Acquisition Model (Adam): A Process Model for Digital Forensic Practice,” J. Digit. Forensics, Secur. Law, 2013, doi: 10.15394/jdfsl.2013.1154.

[11] K. Cabaj, Z. Kotulski, B. Księżopolski, and W. Mazurczyk, “Cybersecurity: trends, issues, and challenges,” Eurasip J. Inf. Secur., vol. 2018, no. 1, pp. 10–12, 2018, doi: 10.1186/s13635-018-0080-0.

[12] oleg kupreev, alexander Gutnikov, and yaroslav shimelev, “Report on DDoS attacks in Q3 2022,” 2022. [Online]. Available: https://securelist.com/ddos-report-q3-2022/107860/.

[13] AWS Shield, “AWS Shield,” 2020. [Online]. Available: https://aws-shield-tlr.s3.amazonaws.com/2020-Q1_AWS_Shield_TLR.pdf.

[14] C. Cimpanu, “AWS said it mitigated a 2.3 Tbps DDoS attack, the largest ever | ZDNET,” Zdnet, 2020. https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-

DOI: https://doi.org/10.29207/resti.v7i5.5153

tbps-ddos-attack-the-largest-ever/.

[15] Sam Kottler, "February 28th DDoS Incident Report," 2018. [Online]. Available: https://githubengineering.com/ddos-incident-report/.

[16] A. Dizdar, "SQL injection attack: Real life attacks and code examples," Retrieved April, 2021. https://brightsec.com/blog/sql-injection-attack/.

[17] T. Moes, "SQL Injection Examples (2023): The 6 Worst Attacks Ever," Software Lab, 2023. https://softwarelab.org/blog/sql-injection-examples/.

[18] M. S. Elsayed, N. A. Le-Khac, S. Dev, and ..., "Ddosnet: A deep-learning model for detecting network attacks," 2020 IEEE 21st …, 2020, [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9217754/.

[19] G. C. Amaizu, C. I. Nwakanma, S. Bhardwaj, J. M. Lee, and D. S. Kim, "Composite and efficient DDoS attack detection framework for B5G networks," Comput. Networks, vol. 188, no. December 2020, p. 107871, 2021, doi: 10.1016/j.comnet.2021.107871.

[20] A. Yudhana, I. Riadi, and F. Ridho, "DDoS classification using neural network and naïve bayes methods for network forensics," International Journal of Advanced Computer Science and Applications, vol. 9, no. 11. pdfs.semanticscholar.org, pp. 177–183, 2018, doi: 10.14569/ijacsa.2018.091125.

[21] F. M. M. Mokbal, W. Dan, A. Imran, L. Jiuchuan, and ..., "MLPXSS: an integrated XSS-based attack detection scheme in web applications using multilayer perceptron technique," IEEE …, 2019, [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8756243/.

[22] D. Chen, Q. Yan, C. Wu, and J. Zhao, "SQL Injection Attack Detection and Prevention Techniques Using Deep Learning," J. Phys. Conf. Ser., vol. 1757, no. 1, 2021, doi: 10.1088/1742-6596/1757/1/012055.

[23] S. Wankhede and D. Kshirsagar, "DoS Attack Detection Using Machine Learning and Neural Network," Proc. - 2018 4th Int. Conf. Comput. Commun. Control Autom. ICCUBEA 2018, 2018, doi: 10.1109/ICCUBEA.2018.8697702.

[24] H. S. Obaid and E. H. Abeed, "Abeed,-DoS and DDoS Attacks at OSI Layers," International Journal of Multidisciplinary Research and Publications Hadeel S. Obaid and Esamaddin H, vol. 2, no. 8. ijmrap.com, pp. 1–9, 2020, [Online]. Available: https://www.researchgate.net/publication/338670829.

[25] S. S. Mohammed et al., "A New Machine Learning-based Collaborative DDoS Mitigation Mechanism in Software-Defined Network," in International Conference on Wireless and Mobile Computing, Networking and Communications, 2018, vol. 2018-Octob, pp. 1–8, doi: 10.1109/WiMOB.2018.8589104.

[26] M. Chambali, A. W. Muhammad, and Harsono, "Classification of Network Packages Based on Statistical Analysis and Neural Network," J. Pengemb. IT, vol. 03, no. 1, pp. 67–70, 2018.

[27] R. Rizal, I. Riadi, and Y. Prayudi, "Network Forensics for Detecting Flooding Attack on Internet of Things (IoT) Device Digital Evidence Cabinets View project eGovernment System and Security related issues View project Network Forensics for Detecting Flooding Attack on Internet of Things (Io," Int. J. Cyber-Security Digit. Forensics, no. September, pp. 382–390, 2018, [Online]. Available: https://www.researchgate.net/publication/327392701.

[28] K. S. Hoon, K. C. Yeo, S. Azam, B. Shunmugam, and F. De Boer, "Critical review of machine learning approaches to apply big data analytics in DDoS forensics," 2018 Int. Conf. Comput. Commun. Informatics, ICCCI 2018, 2018, doi: 10.1109/ICCCI.2018.8441286.

[29] A. Churcher et al., "An experimental analysis of attack classification using machine learning in IoT networks," Sensors (Switzerland), vol. 21, no. 2, pp. 1–32, 2021, doi: 10.3390/s21020446.

[30] M. Alim, I. Riadi, and Y. Prayudi, "Live Forensics Method for Analysis Denial of Service (DOS) Attack on Routerboard," Int. J. Comput. Appl., vol. 180, no. 35, pp. 23–30, 2018, doi: 10.5120/ijca2018916879.

[31] A. Rai, M. M. I. Miraz, D. Das, H. Kaur, and Swati, "SQL Injection: Classification and Prevention," Proc. 2021 2nd Int. Conf. Intell. Eng. Manag. ICIEM 2021, pp. 367–372, 2021, doi: 10.1109/ICIEM51511.2021.9445347.

[32] W. Yang, W. Zuo, and B. Cui, "Detecting Malicious URLs via a Keyword-Based Convolutional Gated-Recurrent-Unit Neural Network," IEEE Access, vol. 7, pp. 29891–29900, 2019, doi: 10.1109/ACCESS.2019.2895751.

[33] Y. Pan et al., "Detecting web attacks with end-to-end deep learning," Journal of Internet Services and Applications, vol. 10, no. 1. Springer, 2019, doi: 10.1186/s13174-019-0115-x.

[34] L. F. Sikos, "Packet analysis for network forensics: A comprehensive survey," Forensic Sci. Int. Digit. Investig., vol. 32, p. 200892, 2020, doi: 10.1016/j.fsidi.2019.200892.

[35] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, and A. Alazab, "Hybrid intrusion detection system based on the stacking ensemble of C5 decision tree classifier and one class support vector machine," Electron., vol. 9, no. 1, 2020, doi: 10.3390/electronics9010173.

[36] W. Pranoto, I. RIadi, and Y. Prayudi, "Live Forensics Method for Acquisition on the Solid State Drive (SSD) NVMe TRIM Function," Kinet. Game Technol. Inf. Syst. Comput. Network, Comput. Electron. Control, vol. 4, pp. 129–138, 2020, doi: 10.22219/kinetik.v5i2.1032.

[37] D. C. Prakoso, I. Riadi, and Y. Prayudi, "Detection of Metasploit Attacks Using RAM Forensic on Proprietary Operating Systems," Kinet. Game Technol. Inf. Syst. Comput. Network, Comput. Electron. Control, vol. 4, pp. 155–160, 2020, doi: 10.22219/kinetik.v5i2.1037.

[38] P. Sharma, D. Arora, and T. Sakthivel, "Enhanced Forensic Process for Improving Mobile Cloud Traceability in Cloud-Based Mobile Applications," Procedia Comput. Sci., vol. 167, pp. 907–917, 2020, doi: 10.1016/j.procs.2020.03.390.

[39] N. Widiyasono, I. A. Dwi Giriantari, M. Sudarma, and L. Linawati, "Detection of Mirai Malware Attacks in IoT Environments Using Random Forest Algorithms," TEM J., no. August, pp. 1209–1219, 2021, doi: 10.18421/tem103-27.

[40] M. Aljabri et al., "Intelligent techniques for detecting network attacks: Review and research directions," Sensors, vol. 21, no. 21, 2021, doi: 10.3390/s21217070.

[41] A. Mihoub, O. Ben Fredj, O. Cheikhrouhou, A. Derhab, and M. Krichen, "Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques," Comput. Electr. Eng., vol. 98, p. 107716, 2022, doi: 10.1016/j.compeleceng.2022.107716.

[42] Dwi Kurnia Wibowo, Ahmad Luthfi, Yudi Prayudi, Erika Ramadhani, and Muhamad Maulana, "Faux Insider Hazard Investigation on Non-Public Cloud Computing by Using ADAM's Technique," J. RESTI (Rekayasa Sist. dan Teknol. Informasi), vol. 6, no. 6, pp. 1028–1036, 2022, doi: 10.29207/resti.v6i6.4714.

[43] W. Yang, M. N. Johnstone, S. Wang, N. M. Karie, N. M. bin Sahri, and J. J. Kang, "Network Forensics in the Era of Artificial Intelligence," Studies in Computational Intelligence, vol. 1025. Springer International Publishing, pp. 171–190, 2022, doi: 10.1007/978-3-030-96630-0_8.

[44] M. Maabreh, I. Obeidat, E. A. Elsoud, A. Alnajjai, R. Alzyoud, and O. Darwish, "Towards Data-Driven Network Intrusion Detection Systems: Features Dimensionality Reduction and Machine Learning," Int. J. Interact. Mob. Technol., vol. 16, no. 14, pp. 123–135, 2022, doi: 10.3991/ijim.v16i14.30197.

[45] I. Riadi, A. Yudhana, and Galih Pramuja Inngam Fanani, "Comparative Analysis of Forensic Software on Android-based MiChat using ACPO and DFRWS Framework," J. RESTI (Rekayasa Sist. dan Teknol. Informasi), vol. 7, no. 2, pp. 286–292, 2023, doi: 10.29207/resti.v7i2.4547.

[46] S. Hidayatulloh and D. Saptadiaji, "Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP)," J. Algoritm., vol. 18, no. 1, pp. 77–86, 2021, doi: 10.33364/algoritma/v.18-1.827.

[47] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, and ...,

“A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks,” Electronics, 2019, [Online]. Available: https://www.mdpi.com/558954.

[48] A. Jacobus and E. Winarko, “Penerapan Metode Support Vector Machine pada Sistem Deteksi Intrusi secara Real-time,” IJCCS (Indonesian J. Comput. Cybern. Syst., vol. 8, no. 1, p. 13, 2014, doi: 10.22146/ijccs.3491.

[49] M. Shen, X. Tang, L. Zhu, X. Du, and M. Guizani, “Privacy-Preserving Support Vector Machine Training over Blockchain-Based Encrypted IoT Data in Smart Cities,” IEEE Internet Things J., vol. 6, no. 5, pp. 7702–7712, 2019, doi: 10.1109/JIOT.2019.2901840.

[50] F. G. Deriba, A. O. Salau, S. H. Mohammed, T. M. Kassa, and W. B. Demilie, “Development of a Compressive Framework Using Machine Learning Approaches for SQL Injection Attacks,” Prz. Elektrotechniczny, vol. 98, no. 7, pp. 181–187, 2022, doi: 10.15199/48.2022.07.30.

[51] P. Roy, R. Kumar, and P. Rani, “SQL Injection Attack Detection by Machine Learning Classifier,” Proc. - Int. Conf. Appl. Artif. Intell. Comput. ICAAIC 2022, no. May, pp. 394–400, 2022, doi: 10.1109/ICAAIC53929.2022.9792964.

[52] Q. Li, W. Li, J. Wang, and M. Cheng, “A SQL Injection Detection Method Based on Adaptive Deep Forest,” IEEE Access, vol. 7, pp. 145385–145394, 2019, doi: 10.1109/ACCESS.2019.2944951.

[53] P. Tang, W. Qiu, Z. Huang, H. Lian, and G. Liu, “Detection of SQL injection based on artificial neural network,” Knowledge-Based Syst., vol. 190, p. 105528, 2020, doi: 10.1016/j.knosys.2020.105528.

[54] I. S. Crespo-Martínez, A. Campazas-Vega, Á. M. Guerrero-Higueras, V. Riego-DelCastillo, C. Álvarez-Aparicio, and C. Fernández-Llamas, “SQL injection attack detection in network flow data,” Comput. Secur., vol. 127, 2023, doi: 10.1016/j.cose.2023.103093.

[55] J. Mack, Y.-H. (Frank) Hu, and M. A. Hoppa, “A Study of Existing Cross-Site Scripting Detection and Prevention Techniques Using XAMPP and VirtualBox,” Va. J. Sci., vol. 70, no. 3, p. 1, 2019, doi: 10.25778/bx6k-2285.

[56] F. A. Mereani and J. M. Howe, “Detecting Cross-Site Scripting Attacks Using Machine Learning,” Advances in Intelligent Systems and Computing, vol. 723. Springer International Publishing, pp. 200–210, 2018, doi: 10.1007/978-3-319-74690-6_20.

[57] D. Korac, B. Damjanovic, and D. Simic, “Information Security in M-learning Systems: Challenges and Threats of Using Cookies,” 2020 19th Int. Symp. INFOTEH-JAHORINA, INFOTEH 2020 - Proc., no. March, pp. 18–20, 2020, doi: 10.1109/INFOTEH48170.2020.9066344.

[58] K. Vijayalakshmi and E. Syed Mohamed, “Case Study: Extenuation of XSS Attacks through Various Detecting and Defending Techniques,” J. Appl. Secur. Res., vol. 16, no. 1, pp. 91–126, 2021, doi: 10.1080/19361610.2020.1735283.

[59] G. Xu et al., “JSCSP: A Novel Policy-Based XSS Defense Mechanism for Browsers,” IEEE Trans. Dependable Secur. Comput., vol. 19, no. 2, pp. 862–878, 2022, doi: 10.1109/TDSC.2020.3009472.

[60] R. W. Kadhim and M. T. Gaata, “A hybrid of CNN and LSTM methods for securing web application against cross-site scripting attack,” Indones. J. Electr. Eng. Comput. Sci., vol. 21, no. 2, pp. 1022–1029, 2020, doi: 10.11591/ijeecs.v21.i2.pp1022-1029.

[61] D. Faroek, Rusydi Umar, and Imam Riadi, “Classification Based on Machine Learning Methods for Identification of Image Matching Achievements,” J. RESTI (Rekayasa Sist. dan Teknol. Informasi), vol. 6, no. 2, pp. 198–206, 2022, doi: 10.29207/resti.v6i2.3826.

[62] M. Batta, “Machine Learning Algorithms - A Review,” Int. J. Sci. Res., vol. 18, no. 8, pp. 381–386, 2018, doi: 10.21275/ART20203995.

[63] E. S. Pilli, R. C. Joshi, and R. Niyogi, “A Generic Framework for Network Forensics,” Int. J. Comput. Appl., vol. 1, no. 11, pp. 1–6, 2010, doi: 10.5120/251-408.