# Model Design of Intrusion Detection System on Web Server Using Machine Learning Based

Agus Tedyyana[1,2], Osman Ghazali[3], Onno W. Purbo[4]

{agustedyyana@polbeng.ac.id, osman@uum.edu.my, onno@indo.net.id}

Department of Informatic Engineering, Politeknik Negeri Bengkalis, 28711, Indonesia[1]
School of Computing, College of Arts and Sciences, Universiti Utara Malaysia, Sintok, Kedah 06010, Malaysia[2,3]
Department of Informatic, Institute Technology Tangerang Selatan, Kota Tangerang Selatan, Banten 15117, Indonesia[4]

**Abstract**. In the current era of information technology development, web server security has become a primary concern in maintaining data integrity, confidentiality, and availability. With the emergence of increasingly complex and evolving cyber threats, Intrusion Detection Systems (IDS) play a crucial role in addressing these challenges. In this research, we propose an innovative approach to enhance web server security by implementing an Intrusion Detection System empowered with Machine Learning Algorithms. In the pursuit of enhancing web server security, this research delves into designing an Intrusion Detection System (IDS) empowered by Machine Learning (ML). The foundation of this approach hinges on transparent public datasets, subjected to intensive pre-processing steps such as data cleaning, normalization, and feature selection. After refining, the data steers ML algorithms to discern potential cyber threats from standard patterns. The novel ML-based IDS showcases an ability superior to traditional systems, with the prowess to differentiate between benign and malicious activities. A salient feature of this IDS is its real-time alert mechanism on Telegram, ensuring immediate notification to security teams upon potential breach detection. Comparative results accentuate the model's enhanced accuracy and a significant reduction in false alarms. This study substantiates the utility of ML in elevating cybersecurity measures and paves the way for deeper investigations into advanced web server protective mechanisms.

**Keywords***:* Intrusion Detection Systems, web server, Machine Learning, feature selection, Anomaly Detection

## 1 Introduction

In recent decades, the growth of the Internet in Indonesia has been significant. According to the Indonesian Internet Service Provider Association (APJII), internet penetration in the country has reached over 78% of the total population. This digital transformation has permeated not just among the youth but also other population segments who use the internet for communication, shopping, education, entertainment, and other necessities.

ABEC 2023, September 21, Bengkalis, Indonesia

DOI 10.4108/eai.21-9-2023.2342879

One of the factors driving internet growth in Indonesia is easy access through mobile devices. Advancements in telecommunications technology, especially 4G and 5G, coupled with the increasing affordability of smartphones, have enabled the broader population to connect with the virtual world. This phenomenon has been further boosted by the emergence of various local digital platforms such as Gojek, Tokopedia, and Bukalapak, which cater to diverse societal needs. However, alongside this rapid development, Indonesia also faces significant challenges in the form of cyber threats. As online activity has grown, the threats from cybercriminals have also increased.

The National Cyber and Crypto Agency (BSSN) reported that cybercrime in Indonesia has seen a substantial rise in recent years. From phishing, ransomware, and defacement to DDoS attacks, these are among the threats frequently encountered by Indonesian internet users. These attacks often result in substantial financial losses and tarnish the reputations of institutions or individuals targeted. One particularly alarming incident was when several government websites were hacked and defaced. This incident was concrete evidence that cyber threats could target anyone, including institutions with substantial resources.

The vulnerability stems from a lack of public awareness about the importance of cyber security[1]. Many internet users still employ easily guessable passwords or use the same password across multiple platforms. Additionally, a lack of knowledge about tactics used by cybercriminals, such as phishing techniques, makes users susceptible[2]. Another challenge comes from infrastructure and regulations that aren't entirely supportive. Although the government has made significant strides by issuing various regulations and policies related to cybersecurity, their implementation, and socialization still take time. Addressing these threats requires a collaborative approach involving the government, the private sector, the IT community, and the general public. Enhancing digital literacy and cybersecurity awareness needs to be undertaken on a broad scale to protect the public better while surfing the web[3].
In this context, an Intrusion Detection System (IDS) becomes very important[4]. IDS functions to detect and provide warnings against any suspicious attempts or attacks aimed at a system, including web servers. However, with the development of technology and increasingly sophisticated attack methods, traditional IDS often have difficulty identifying new attacks or attacks using disguise techniques[5].

One promising solution in overcoming the limitations of traditional IDS is the application of Machine Learning (ML) technology[6]. Machine learning is a branch of computer science that focuses on developing algorithms that enable computers to learn and make decisions based on data. In the last decade, the development of machine learning has reached a stage where it can be applied in various fields, including cybersecurity.

In the context of IDS, machine learning can be "taught" to identify suspicious network traffic patterns more accurately and adaptively. For example, through a training process with historical data, ML models can recognize attacks that have never been seen before based on similarities to known attack patterns. In addition, the adaptability of ML allows IDS to continuously "learn" from the latest attacks and update its knowledge base[7].
However, implementing ML in IDS also brings its challenges, such as selecting the right features, the need for large data training, and the risk of overfitting. Nonetheless, with the right approach, ML has the potential to significantly increase the effectiveness of IDS, especially in dealing with evolving cybersecurity threats. In this article, we will discuss more how machine

learning can be applied in IDS to improve web server security and the challenges and opportunities that lie ahead [8].

## 2 Research Methods

Given the aim of enhancing intrusion detection systems on web servers using a machine-learning approach, our research methods encompass a multifaceted study of related works, understanding the broader cyber threat landscape, delving into the specifics of web servers, the principles of intrusion detection, the mechanics of machine learning, and the relevance of feature selection. Here's a structured breakdown:

### 2.1. Internet and Threats

The modern era is marked by the unprecedented growth of the Internet, rendering borders obsolete in the digital realm and connecting billions of devices worldwide. The Internet's rise is not just a technological phenomenon; it represents a transformation of societies, economies, and individual lives, enabling a global exchange of ideas, commerce, and culture. However, with the Internet's remarkable capabilities come significant threats that challenge its users' integrity, safety, and privacy[9].

As Internet adoption has surged, so has the sophistication and volume of cyber threats. Cybercriminals consistently explore vulnerabilities in systems, applications, and even human behaviour. The threat spectrum spans from relatively harmless spam emails to highly destructive ransomware attacks, data breaches, and advanced persistent threats[10], [11]

The rapid digitalization in Indonesia, characterized by a booming e-commerce market, growing tech startups, and increasing governmental digital services, makes the nation a notable target for cyber threats. Indonesia's cyber landscape has witnessed rising incidents of phishing, web defacements, and ransomware attacks. Additionally, as local businesses migrate to cloud-based platforms and offer digital services, their web servers become potential targets, underscoring the need for robust intrusion detection mechanisms[12].

### 2.2. Web Server

A web server is a system that processes incoming network requests over HTTP (Hypertext Transfer Protocol) and several other related protocols. Its primary function is to store, process, and deliver web pages to users[13], [14]. When someone accesses a website, they're effectively communicating with the web server, requesting it to serve up the required web pages. Web servers can be hardware or software-based. Popular web server software includes Apache, Nginx, Microsoft's Internet Information Services (IIS), and LiteSpeed[15], [16].

Web servers, given their essential role and accessibility, are frequent targets for cyber-attacks. Here are some common threats to web servers: DDoS Attacks: Distributed Denial of Service attacks aim to flood the server with unnecessary requests, overloading its capacity and making it unavailable to legitimate users[17], [18]. SQL Injection: Attackers manipulate a site's database by inputting malicious SQL statements in input fields, potentially leading to unauthorized viewing of data, corrupting or deleting data, and other malicious activities[19], [20]. Cross-Site Scripting (XSS): This occurs when malicious scripts are injected into web pages viewed by

users. The scripts can then steal information and send it to the attacker[21]. Brute Force Attacks: Here, attackers use trial-and-error methods to guess the right credentials (like username and password) to gain unauthorized access.

The integral role of web servers in the digital infrastructure combined with their public-facing nature makes them a significant target for cyber threats. Protection goes beyond just regular updates; it also requires proactive monitoring and the implementation of security protocols, including advanced solutions like machine learning-enhanced Intrusion Detection Systems, to detect and respond to threats in real-time. As cyber threats continue to evolve, so must the defences put in place to protect these vital digital gateways.

### 2.3. Intrusion Detection System

An Intrusion Detection System, commonly known as IDS, is either a specialized device or a software application tasked with monitoring a network or system for any signs of malicious activity or policy breaches. Acting as the digital world's counterpart to a security surveillance system, an IDS continually scans and evaluates activities to detect potential cyber threats, subsequently producing detailed reports to a designated management station. These reports serve as a vital tool, offering administrators and security professionals valuable insights into potential vulnerabilities or ongoing attacks[6].

Intrusion Detection Systems can be broadly categorized into different types based on their operation and deployment. Network-based Intrusion Detection Systems (NIDS) primarily focus on monitoring and evaluating network traffic, identifying any suspicious or unconventional behaviour. Strategically placed at network choke points, NIDS can oversee vast segments of a network. In contrast, Host-based Intrusion Detection Systems (HIDS) concentrate on individual hosts, often zeroing in on servers. They are responsible for monitoring both inbound and outbound packets, ensuring that the host remains free from any malicious activities[4], [22].
IDS solutions can also differ in their method of detecting threats. Signature-based IDS operates by recognizing known patterns of malicious behaviour, such as particular byte sequences in network traffic or familiar harmful instruction sequences used by malware. On the other hand, anomaly-based IDS defines its operation by comparing detected activities against a predefined baseline representing "normal" behaviour. Any deviation from this norm raises a red flag.

A typical IDS operates in a relatively straightforward manner. It begins with active data collection, sourcing information either from network traffic or individual system activities. Once sufficient data has been amassed, the IDS transitions into the analysis phase. Depending on its underlying detection method, either signature-based or anomaly-based, it sifts through the data to pinpoint any suspicious activities. If the IDS identifies a potential threat, it immediately alerts the network or system administrators. Depending on its sophistication and the perceived threat level, some IDS solutions can even initiate a response to detected threats, ranging from blocking malicious IP addresses to shutting down affected network portions to contain a potential breach[23], [24].

However, as formidable as IDS solutions might sound, they are not without their challenges. They can sometimes misinterpret legitimate traffic or activities as harmful, leading to false positives. These unnecessary alerts can cause unwarranted panic or potential service disruptions. More concerning is the possibility of false negatives, where actual malicious activities slip

through undetected. Maintaining an IDS, especially across vast networks, can be resource-intensive, potentially slowing down other vital processes. Attackers, well aware of IDS functionalities, constantly innovate, developing evasion techniques like packet fragmentation or payload encryption to bypass detection.

### 2.4. Machine Learning

Machine Learning (ML) has revolutionized a myriad of sectors in the contemporary digital ecosystem, from healthcare to finance, and its importance cannot be understated when discussing cybersecurity and intrusion detection. At its core, machine learning is a subset of artificial intelligence that employs algorithms allowing computers to learn and make decisions or predictions from data without explicit programming[25], [26].

The foundational concept behind machine learning is straightforward: given a sufficient amount of data, a machine can be "taught" to recognize patterns and make informed decisions based on them. There are several categories of machine learning, each with its unique strengths: Supervised Learning: The most prevalent category, involves teaching the machine using labelled data. In essence, both the input and desired output are provided, and over time, the machine fine-tunes its algorithm to get closer to the expected results[27]. Unsupervised Learning: Unlike supervised learning, unsupervised methods don't use labelled data. Instead, they rely on clustering and association to understand and process inputs[28]. Reinforcement Learning: Here, the algorithm learns by interacting with an environment and receiving feedback (rewards or penalties) based on its actions[29].

How does machine learning intersect with cybersecurity and intrusion detection? Traditional Intrusion Detection Systems (IDS) operate on pre-defined signatures or known attack patterns. However, in a rapidly evolving threat landscape, relying solely on known attack vectors is insufficient. Here, machine learning proves invaluable[4], [30]. By employing machine learning algorithms, IDS can adapt and learn from the vast amount of network traffic data, recognizing and responding to novel attack patterns never seen before. For example, an anomaly-based IDS, augmented with machine learning capabilities, can establish a "baseline" of what constitutes normal network traffic. Over time, it becomes proficient at detecting deviations from this norm, flagging them for review or responding instantly. This dynamic approach is especially potent against zero-day vulnerabilities or advanced persistent threats that elude traditional detection methods. Furthermore, with the surge in the volume of data flowing across networks, manual monitoring becomes an unfeasible task. Machine learning algorithms can sift through petabytes of data, identifying potential threats with precision and speed that no human analyst can match.

### 2.5. Feature Selection

Feature selection, a pivotal process in machine learning, directly influences the performance and efficacy of models, especially when the objective is as critical as intrusion detection. In the context of machine learning, features are individual measurable properties or characteristics of the phenomena being observed. In intrusion detection, these features could range from packet lengths and connection durations in network traffic, to more abstract features like user behavior patterns. However, not all features are created equal. While some carry significant information and can aid a model in making accurate predictions, others add noise, or at best, are redundant. It's here that the process of feature selection becomes indispensable[31].

The primary objectives of feature selection are: Improving Model Performance: By discarding irrelevant or redundant features, models often perform better, as they're less likely to overfit the noise in the data. This results in more accurate and generalizable models. Reducing Computational Load: Fewer features mean less data to process, which translates to faster training times and reduced memory and computational requirements. This can be especially beneficial when deploying models in real-time environments, such as live web servers. Enhancing Model Interpretability: A model that utilizes fewer, more relevant features is often easier to understand and interpret. This can be crucial in cybersecurity contexts, where understanding the rationale behind a model's decision can aid in refining defence strategies[32], [33].

When it comes to intrusion detection, the significance of feature selection is further amplified. Web servers and network environments generate vast amounts of data, with myriad potential features. The challenge is identifying which of these features are most indicative of malicious activity. By selecting the right features, an Intrusion Detection System (IDS) augmented with machine learning can more effectively discern between benign and malicious traffic, reducing false positives and ensuring genuine threats don't slip through undetected. In conclusion, feature selection is not just a beneficial step but an imperative one in the context of machine learning for intrusion detection. By focusing on the most relevant signals and discarding noise, it ensures that models are both efficient and effective, ready to face the multifaceted threats that modern web servers encounter.

# 3 Result and Discussion

## 3.1. Generate Model Machine Learning

Developing an Intrusion Detection System for web servers using a Machine Learning model begins with a clear understanding of the objective: proactively and adaptively identifying and responding to potential security threats. Central to this endeavour is the use of public datasets. These datasets, known for their accessibility, diversity, and transparency, often encompass a range of recorded attacks, giving insights into the appearance of malicious activities versus regular traffic.

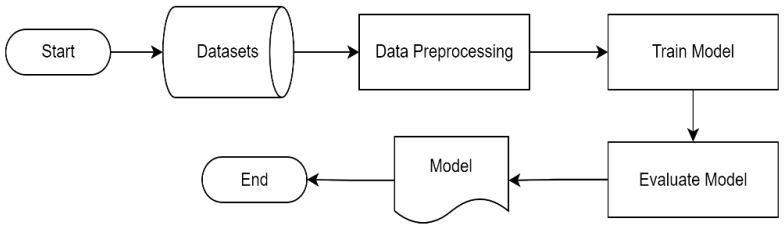


**Fig. 1.** Model Machine Learning

Figure 1. The following Machine Learning Model explains each stage. Before data becomes a tool in the learning process, it undergoes a stage known as pre-processing. This stage involves refining the dataset by eliminating redundancies, dealing with missing data, normalizing features, and selecting the most important attributes for intrusion detection. Once the data is

prepped and prepared, the actual model training begins. The data set is fed into selected machine learning algorithms, allowing the model to 'learn' and make predictions or classifications based on visible patterns. However, simply training a model doesn't suffice. Its efficacy needs validation. The model's real-world performance in detecting intrusions can be gauged using a separate set of data not previously exposed to the model during training. Metrics like accuracy, precision, recall, and the F1 score provide insights into how well the model performs under real-world scenarios.

### 3.2. Prepocessing

Preprocessing plays a pivotal role in shaping the data, ensuring that machine learning models are fed with quality inputs that drive optimal performance. The journey of data refinement begins with cleaning missing values. In any dataset, gaps or omissions can often introduce bias or inaccuracies. To tackle this, one identifies these missing segments and decides on an approach to address them. It could involve filling in those voids using imputation techniques, where values such as the mean or median of a column replace the missing spots. At times, eliminating certain rows or columns altogether might make sense.


**Fig. 2.** Preprocessing Phase

Figure 2. The following Preprocessing Phase explains each stage Once the data is free from gaps, the next step is to ensure that it speaks the language machines understand best: numbers. Many datasets come with labels that might be descriptive. In the context of intrusion detection systems (IDS), these labels might represent various types of network behaviours. Such categorical labels need translation into a numerical format, a process known as label encoding. For instance, if our IDS dataset contains labels like 'Benign', 'Attack', and 'Suspicious', each would get a unique numerical identifier.

Having prepared the data structure, it's time to set the stage for the actual modelling. But before diving into it, it's crucial to earmark portions of the data for different purposes. The dataset is usually split, with a majority, say 80%, being utilized to train the model, while the remaining 20% stands by to test the model's prowess later.

### 3.3. Implementation Model to IDS

Once the process is initiated, the custom model is activated. These models, designed with unique capabilities to recognize and categorize various digital behaviours, are then loaded into our Intrusion Detection System (IDS). The primary role of this IDS is to continuously monitor and review our web server logs, which in turn act as a digital diary of all the traffic and activity that occurs on our platform.

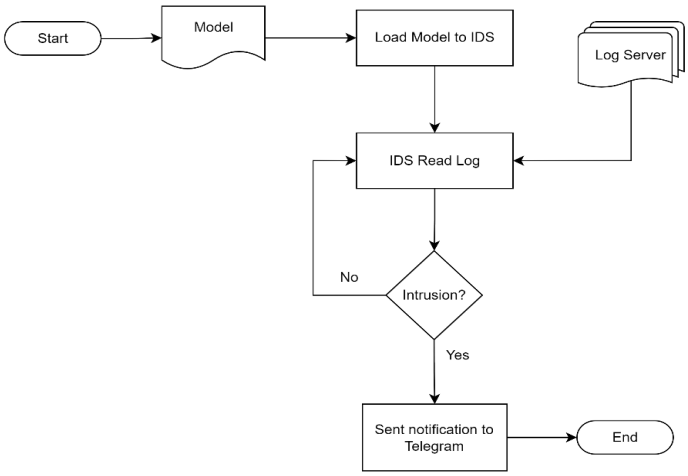


**Fig. 3.** Load Model to IDS

Figure 3 The Load to IDS model explains that the IDS here is not just any ordinary monitoring system. Empowered by the model to distinguish between regular and potentially hazardous activities. With every passing second, it meticulously scans every line of the log, making judgments as to whether an activity is harmless or poses a potential threat.

And this is where his brilliance really shines. If our IDS, with the help of the model, identifies any activity that appears to be an intrusion or a malicious attempt to infiltrate our system, it immediately triggers an alert mechanism. This is not just any warning. It sends real-time notifications to our dedicated Telegram channel. The instantaneous nature of Telegram ensures that our security team picks up on these alerts immediately, allowing them to take swift action to neutralize any threats.

## 4 Conclusion

The initial step to creating an IDS via ML entails utilizing public datasets known for their transparency. It undergoes a rigorous pre-processing phase before the data is ready for model training. this involves data cleaning, normalization, and feature selection. Once primed, the data feeds the chosen ML algorithms, trained to identify potential threats based on discernible patterns. Furthermore, model validation ensures its efficiency in real-world scenarios. pre-processing is cardinal to the success of the model. This phase initiates with data cleaning, particularly addressing missing values through imputation or omission. Subsequently, categorical labels in the dataset transform into numerical equivalents (label encoding).

IDS Model Implementation: The post-training phase sees the integration of the custom ML model into the Intrusion Detection System. Unlike conventional systems, this IDS discerns between benign and potentially malevolent activities. When the IDS perceives any hint of a cyber breach, it instantaneously triggers alerts on a dedicated Telegram channel. The immediacy

of this alert system ensures that security teams are promptly notified, enabling them to address potential threats without delay.

In the relentless battle against cyber threats, integrating Machine Learning algorithms into Intrusion Detection Systems offers a promising avenue to bolster web server security. This research underlines the efficacy of such a system, demonstrating a marked reduction in false positives and heightened accuracy in intrusion detection compared to traditional methods. As cyber threats continuously morph, staying ahead with dynamic, adaptive systems like the proposed ML-powered IDS becomes imperative. This research not only reinforces the merits of ML in cybersecurity but also sets a foundation for further exploration and refinement in the realm of web server protection.

## References


[1] C. Mehra, A. K. Sharma, and A. Sharma, "Elucidating ransomware attacks in cyber-security," *International Journal of Innovative Technology and Exploring Engineering*, vol. 9, no. 1, pp. 3536–3541, 2019, doi: 10.35940/ijitee.A8106.119119.

[2] M. M. Wrana, M. Elsayed, K. Lounis, Z. Mansour, S. Ding, and M. Zulkernine, "OD1NF1ST: True Skip Intrusion Detection and Avionics Network Cyber-attack Simulation," *ACM Transactions on Cyber-Physical Systems*, vol. 6, no. 4, 2022, doi: 10.1145/3551893.

[3] R. Panigrahi *et al.*, "Intrusion detection in cyber–physical environment using hybrid Naïve Bayes—Decision table and multi-objective evolutionary feature selection," *Comput Commun*, vol. 188, pp. 133–144, 2022, doi: 10.1016/j.comcom.2022.03.009.

[4] A. O. Alzahrani and M. J. F. Alenazi, "ML-IDSDN: Machine learning based intrusion detection system for software-defined network," *Concurr Comput*, vol. 35, no. 1, 2023, doi: 10.1002/cpe.7438.

[5] A. Saritha, B. Ramasubba Reddy, and A. Suresh Babu, "A Hybrid SDN Architecture for IDS Using Bio-Inspired Optimization Techniques," *Journal of Interconnection Networks*, vol. 22, 2022, doi: 10.1142/S0219265921410280.

[6] A. Thakkar and R. Lohiya, "A Review on Machine Learning and Deep Learning Perspectives of IDS for IoT: Recent Updates, Security Issues, and Challenges," *Archives of Computational Methods in Engineering*, vol. 28, no. 4, pp. 3211–3243, 2021, doi: 10.1007/s11831-020-09496-0.

[7] İ. Avcı and M. Koca, "Cybersecurity Attack Detection Model, Using Machine Learning Techniques," *Acta Polytechnica Hungarica*, vol. 20, no. 7, pp. 29–44, 2023, doi: 10.12700/APH.20.7.2023.7.2.

[8] I. P. S. Sethi, S. K. Sinha, N. Chauhan, and D. Khanduja, "Secure Web Application: Rudimentary perspective," *Journal of Engineering Education Transformations*, vol. 36, no. Special Is, pp. 185–190, 2022, doi: 10.16920/jeet/2022/v36is1/22190.

[9] H. Chang and S. Park, "Developing the security threat detection model for the web service using deep neural network," *J Theor Appl Inf Technol*, vol. 98, no. 6, pp. 948–956, 2020.

[10] R. M. Czekster, R. Metere, and C. Morisset, "Incorporating Cyber Threat Intelligence into Complex Cyber-Physical Systems: A STIX Model for Active Buildings," *Applied Sciences (Switzerland)*, vol. 12, no. 10, 2022, doi: 10.3390/app12105005.

[11] M. H. Ali *et al.*, "Threat Analysis and Distributed Denial of Service (DDoS) Attack Recognition in the Internet of Things (IoT)," *Electronics (Switzerland)*, vol. 11, no. 3, 2022, doi: 10.3390/electronics11030494.

[12] R. M. Czekster, R. Metere, and C. Morisset, “Incorporating Cyber Threat Intelligence into Complex Cyber-Physical Systems: A STIX Model for Active Buildings,” *Applied Sciences (Switzerland)*, vol. 12, no. 10, 2022, doi: 10.3390/app12105005.
[13] J. Won-Chi, J. Kim, and N. Park, “Web-Browsing Application Using Web Scraping Technology in Korean Network Separation Application,” *Symmetry (Basel)*, vol. 13, no. 8, p. 1550, 2021, doi: https://doi.org/10.3390/sym13081550.
[14] P. P. Dewani and K. Bains, “WEBACCESSPRO: AN ARTIFICIAL INTELLIGENCE START UP IN CROWDED MARKET,” *Academy of Marketing Studies Journal*, vol. 24, no. 4, pp. 1–17, 2020, [Online]. Available: http://eserv.uum.edu.my/scholarly-journals/webaccesspro-artificial-intelligence-start-up/docview/2516301880/se-2?accountid=42599
[15] H. Chang and S. Park, “Developing the security threat detection model for the web service using deep neural network,” *J Theor Appl Inf Technol*, vol. 98, no. 6, pp. 948–956, 2020, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85083641213&partnerID=40&md5=8ef8b201e6f5f2030f5fd6c80d554713
[16] H. Chang and S. Park, “Developing the security threat detection model for the web service using deep neural network,” *J Theor Appl Inf Technol*, vol. 98, no. 6, pp. 948–956, 2020, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85083641213&partnerID=40&md5=8ef8b201e6f5f2030f5fd6c80d554713
[17] A. Mustapha *et al.*, “Detecting DDoS attacks using adversarial neural network,” *Comput Secur*, vol. 127, 2023, doi: 10.1016/j.cose.2023.103117.
[18] S. Aktar and A. Yasin Nur, “Towards DDoS attack detection using deep learning approach,” *Comput Secur*, vol. 129, 2023, doi: 10.1016/j.cose.2023.103251.
[19] B. Garn, J. Zivanovic, M. Leithner, and D. E. Simos, “Combinatorial methods for dynamic gray-box SQL injection testing,” *Software Testing Verification and Reliability*, vol. 32, no. 6, 2022, doi: 10.1002/stvr.1826.
[20] A. Jesudoss, T. M. Mercy, A. Christy, M. Maheswari, M. Selvi, and V. Ulagamuthalvi, “Analysis and implementation of SQL injection attack and countermeasures using SQL injection prevention techniques,” *International Journal of Engineering Systems Modelling and Simulation*, vol. 13, no. 4, pp. 262–267, 2022, doi: 10.1504/ijesms.2022.126305.
[21] J. Prabakaran, V. Beejawat, S. Goel, and M. Kandarpa, “Cookie poisoning, DNS, XSS testing for web application firewalls,” *International Journal of Advanced Science and Technology*, vol. 29, no. 6 Special, pp. 2533–2537, 2020.
[22] M. J. Babu and A. R. Reddy, “SH-IDS: Specification Heuristics Based Intrusion Detection System for IoT Networks,” *Wirel Pers Commun*, vol. 112, no. 3, pp. 2023–2045, 2020, doi: 10.1007/s11277-020-07137-0.
[23] V. Kanimozhi and T. P. Jacob, “Artificial Intelligence outflanks all other machine learning classifiers in Network Intrusion Detection System on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing,” *ICT Express*, vol. 7, no. 3, pp. 366–370, 2021, doi: 10.1016/j.icte.2020.12.004.
[24] V. Kanimozhi and T. P. Jacob, “Artificial Intelligence outflanks all other machine learning classifiers in Network Intrusion Detection System on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing,” *ICT Express*, vol. 7, no. 3, pp. 366–370, 2021, doi: 10.1016/j.icte.2020.12.004.
[25] A. Shaheed and M. H. D. B. Kurdy, “Web Application Firewall Using Machine Learning and Features Engineering,” *Security and Communication Networks*, vol. 2022, 2022, doi: https://doi.org/10.1155/2022/5280158.
[26] A. Shaheed and H. Al-Radwan, “DASH Framework Using Machine Learning Techniques and Security Controls,” *International Journal of Digital Multimedia Broadcasting*, vol. 2022, 2022, doi: 10.1155/2022/6214830.

[27] M. U. Ilyas and S. A. Alharbi, “Machine learning approaches to network intrusion detection for contemporary internet traffic,” *Computing*, vol. 104, no. 5, pp. 1061–1076, 2022, doi: 10.1007/s00607-021-01050-5.
[28] M. Fatima, O. Rehman, and I. M. H. Rahman, “Impact of Features Reduction on Machine Learning Based Intrusion Detection Systems,” *EAI Endorsed Transactions on Scalable Information Systems*, vol. 22, no. 6, 2022, doi: 10.4108/eetsis.vi.447.
[29] Y. Sugianela and T. Ahmad, “PORTMAP DDOS ATTACK DETECTION USING FEATURE RANK AND MACHINE LEARNING ALGORITHMS,” *ICIC Express Letters, Part B: Applications*, vol. 13, no. 4, pp. 347–354, 2022, doi: 10.24507/icicelb.13.04.347.
[30] M. A. Al-Shareeda, S. Manickam, and M. A. Saare, “DDoS attacks detection using machine learning and deep learning techniques: analysis and comparison,” *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 2, pp. 930–939, 2023, doi: 10.11591/eei.v12i2.4466.
[31] K. G. Maheswari, C. Siva, and G. Nalinipriya, “Optimal cluster based feature selection for intrusion detection system in web and cloud computing environment using hybrid teacher learning optimization enables deep recurrent neural network,” *Comput Commun*, vol. 202, pp. 145–153, 2023, doi: 10.1016/j.comcom.2023.02.003.
[32] V. Lakhno *et al.*, “EXPERIMENTAL STUDIES OF THE FEATURES OF USING WAF TO PROTECT INTERNAL SERVICES IN THE ZERO TRUST STRUCTURE,” *J Theor Appl Inf Technol*, vol. 100, no. 3, pp. 705–721, 2022.
[33] M. Hasnain, S. R. Jeong, M. F. Pasha, and I. Ghani, “Performance anomaly detection in web services: An RNN-based approach using dynamic quality of service features,” *Computers, Materials and Continua*, vol. 64, no. 2, pp. 729–752, 2020, doi: 10.32604/CMC.2020.010394.