INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Artificial Intelligence Based Multi-Layer Approach for Finding Unknown Attacks in Cloud Network by Using Hybrid Intrusion Detection

D Rajagopal[1]*, K Padmanabhan[2]

1 Research Scholar and Assistant Professor, PG and Research Department of Computer Science and Applications, Vivekanandha College of Arts and Sciences for Women (Autonomous), Tiruchengode, Namakkal Dt, Tamil Nadu, India
2 Professor, PG and Research Department of Computer Science and Applications, Vivekanandha College of Arts and Sciences for Women (Autonomous), Tiruchengode, Namakkal Dt, Tamil Nadu, India

OPEN ACCESS

Received: 08-07-2024

Accepted: 10-08-2024

Published: 28-08-2024

Citation: Rajagopal D, Padmanabhan K (2024) Artificial Intelligence Based Multi-Layer Approach for Finding Unknown Attacks in Cloud Network by Using Hybrid Intrusion Detection. Indian Journal of Science and Technology 17(35): 3643-3652. https://doi.org/10.17485/IJST/v17i35.2209

* **Corresponding author**.

sakthiraj2782007@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: The objective of this study is to explore Intrusion Detection Systems and their various types by gathering research from previously published articles in refereed journals. The focus is on developing a proposed model capable of identifying unknown attacks in cloud networks using Signature and Anomaly-based Intrusion Detection Systems. Subsequently, the efficiency of the proposed model will be assessed, and a comparison with existing models will be conducted. The paper's main objective is to identify unknown attacks in a cloud network using a combination of signature and anomaly-based intrusion detection systems in an artificial intelligence-based multi-layered approach. **Methods:** Leveraging insights from existing literature, the proposed model combines signature-based IDS for known threat detection and anomaly-based IDS for detecting unusual behavioral patterns indicative of new or unseen attacks. Experimental evaluations using NSL-KDD and ADFA datasets demonstrate competitive accuracy and detection rates, with the proposed artificial intelligence-based Hybrid IDS achieving high performance in detecting both normal and malicious activities. **Findings:** This model produces above 90%, 96%, and 98% efficiency in the wired, Wireless, and Cloud networks respectively, and this model finds known attacks effectively while using parameters like event logs, file transferring time, TCP and UDP addresses, CPU Usage, Weak and synthetic data, IP and MAC address. Existing literature said that the existing model using the Hybrid Intrusion detection model can identify unknown attacks with a maximum of 80%, 92%, and 96% accuracy respectively. The findings suggest that the artificial intelligence-based multi-layered approach offers a promising solution for enhancing cloud network security, with the potential for further optimization and integration of advanced technologies in future research endeavors. **Novelty:** This study presents an artificial intelligence-based multi-layered approach for detecting unknown

attacks in cloud networks by integrating signature-based and anomaly-based intrusion detection systems (IDS). The authors developed the model to detect the intrusion by using the Behaviour Profiling algorithm and dynamically prevent the data from intrusion by using the Statistical approach model. The authors trying to find unknown attacks, therefore the authors defined the objective of this paper as to find the unknown attacks in cloud networks by using the combination of signature and anomaly-based intrusion detection systems. The objective is to develop a model capable of effectively identifying cyber threats in cloud environments. The existing models do not concentrate on identifying unknown attacks by using Signature-based Intrusion Detection. Very few of the literature said that known attacks can be identified easily by using Signature-based Intrusion Detection but the unknown attacks identifying process is hard. Some of the Literature said that using the Hybrid Intrusion detection model can identify unknown attacks with a maximum of 80%, 92%, and 96% accuracy respectively. The current paper identifies unknown attacks in the cloud network using a combination of signature and anomaly-based intrusion detection systems in an artificial intelligence-based multi-layered approach and it produced above 97% accuracy. The unique feature of the model is artificial intelligence-based multi-layered approach and dynamic key have been utilized to avoid malicious activities in the network.

Keywords: Anomaly based IDS; Cloud Network Security; Hybrid IDS; Multi-Layer Approach; Signature based IDS

1 Introduction

Due to the increase in the number of Internet users and the digitalization of society, cyber incidents and cyber-attacks are increasing. Intrusion activity may deviate slightly from the norm and is sometimes difficult to distinguish. Today, businesses recognize the importance of using firewalls to protect valuable information and internal resources from unauthorized access[(1)]. Intrusion detection systems have become an important component to ensure system and network security[(1)]. The main task of intrusion detection systems in networks is to support computer systems in preparing for and responding to network attacks.

The following content has described the existing published papers survey. They are, comparing the efficacy of signature-based detection techniques; a study was carried out that focused on the use of process analysis to identify threats in industrial control infrastructure systems. The study aims to identify hidden processes in industrial control device protocols and identify real-time behavior-based attacks by analyzing a pattern called "Capturing the Invisible (CTI)". This study included a recognition algorithm[(2)]. Discussed different Signature-based Intrusion Detection systems and their advantages while using signatures and patterns in the model to acquire the Intrusion Detection Systems' features which have been used by the administrators to identify the threats and cyber-attacks in the computer system. They promised that 80% of the incidents were detected using the model and event behavior of the user have identified the deviations and decided the traffic to flag[(3)]. Provides awareness to the users on intrusions and secured operations on malicious activities in Android phones and the systems developed by using object-oriented analysis and design method (OOADM) and log entries for more flexibly and efficiently[(4)]. Deployed Suricata IDPS by using the NN model, metaheuristic-based feature selection, fuzzy logic, and the latest stable version of Kali Linux 2020.3 for avoiding attacks in web applications which has achieved 96.11%

accuracy[5]. Proposed anomaly detection model by using machine learning (ML) algorithms and statistical analysis[6]. Provides intelligent cyber security systems that have been developed by using Field Programmable Gate Arrays[7].

Through the above survey, the research gap was identified. The existing models do not concentrate on identifying unknown attacks by using Signature-based Intrusion Detection. Very few of the literature said that known attacks can be identified easily by using Signature-based Intrusion Detection but unknown attacks process is hard. Some of the Literature said that using the Hybrid Intrusion detection model can identify unknown attacks with a maximum of 80%, 92%, and 96% accuracy respectively. The current paper identifies unknown attacks in the cloud network using a combination of signature and anomaly-based intrusion detection systems in an artificial intelligence-based multi-layered approach and it produced above 97% accuracy. The unique feature of the model is artificial intelligence-based multi-layered approach and dynamic key have been utilized to avoid malicious activities in the network.

1.1 Intrusion Detection System

”Intrusion” is defined as unauthorized entry into someone else’s space or property. However, these actions are intended to violate confidentiality, integrity, and privacy- the three main security objectives of computer networks in the field of computer science[8]. IDS (Intrusion Detection System) is a combination of hardware and software systems that is used to detect attacks on computer systems and then react to maintain security and confidentiality. In addition, it supports monitoring the behavior of the users, inspecting operations performed by the user in the system, and identifying normal and abnormal activities[3]. An Intrusion Detection System is a hardware or software that keeps an eye on a network for unauthorized or harmful behavior[9]. Systems possess the ability to thwart infiltration attempts, it is not a necessary or anticipated feature for surveillance systems[8]. These systems can be purchased as hardware or software. In order to safeguard their data from these attacks, network administrators can take the necessary precautions after receiving alerts from IDS about malicious activity occurring within the network[4]. An intrusion detection system, by these several definitions, is a software application that is incorporated into hardware to stop illegal activities on a network and safeguard data by sending alarms to administrators delivered by the software[10].

1.2 Classification of IDS

In addition, some IDS technologies have the ability to log which events are audited for further analysis or to combine the events with other data to determine the best course of action for mitigation. This type of information reflects an assault based on the environment of the system that is being threatened because it is extremely sensitive to the application’s operating system, version, and usage. In general, network traffic, system calls, phase-oriented in entity-level applications, audit or logs, and device or user activity are some of the several sources from which IDS gathers data.

There are two essentially important intruder alarm systems that rely on the specific workplace and procedure. These are: IDS can be categorized as Host-based, Network-based, Anomaly-based, Signature-based, Specification-based, Hybrid, and Signature-based depending on how they are composed and function. Email, spam, Trojan horses, viruses, and other network-related packet flow are among the things that are captured by NIDS components[11]. In contrast, HIDS scans file accesses and events linked to programs. AIDS concluded that such activity represents an attack by comparing it to both regular and abnormal behavior on the network. SIDS employs criteria for threat identification while operating in the context of comparing packet contents with indications of viruses. The immune system component linked to immune cell adhesion is affected by SPECIDS, much like in the case of AIDS. HyIDS is created by combining the Packet Header Anomaly Detection (PHAD), which functions as a pre-processor, with the Network Traffic Anomaly Detection (NETAD), which detects packets based on unusual byte patterns that are started at the packets that are streaming over the network. The first and second research strategies signature-based intrusion detection and anomaly-based intrusion detection, respectively were selected for this aim. For this reason, the next chapter describes these intrusion detection methods and also offers an implementation procedure guide.

Particularly, the authors of this paper sought to investigate cloud networks by employing attack detection systems based on strings to identify threats. The signature-based intrusion detection system (IDS) is a widely utilized approach for threat identification due to its ease of installation[12]. A database containing the infected or damaged patterns or signatures present in the IDS is consulted in order to perform a more thorough identification of network packets[13]. In actuality, it is utilized to search for a pattern that is genuinely sought after in a certain type of data packet. These signatures may be located at radically different locations inside the data packet, contingent upon the particular sort of assault. Regarding signature-based detection, a network assault can be identified because each signature is unique. Accordingly, it analyzes if the present activity, transactions, traffic, or behavior in Signature-based NIDS is related to an event pattern that is comparable to the dangers that are already in place[14]. Simply put, the goal of a signature-based intrusion detection system (IDS) is to determine whether a particular packet

matches one of its signatures. If so, it forwards the packet to an analytical backend [4].

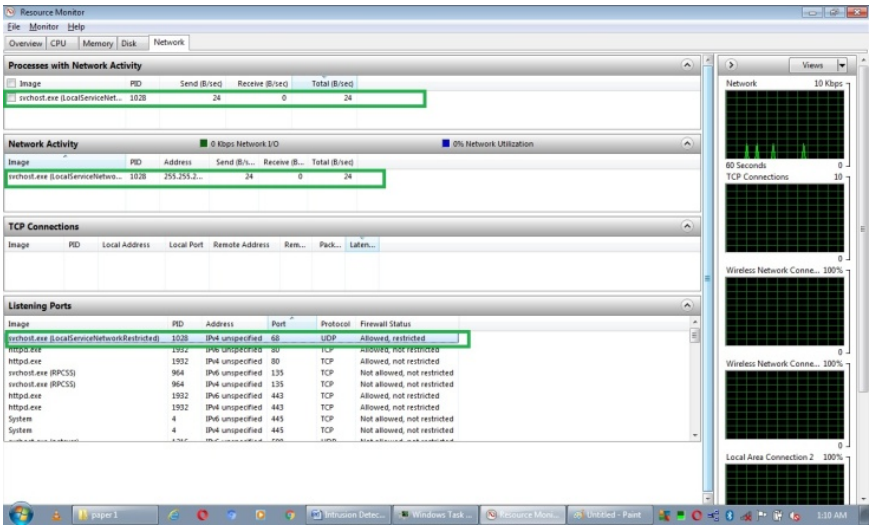

Fig 1. Network tab in Resource Monitor

The majority of current global signature-based intrusion detection systems (IDSs) either use regular expression matching approaches or precisely match strings. Attacks that are both metamorphic and polymorphic are common. In these assaults, the attacker creates new signatures that can defeat established systems. Matching input packets that enter the system right away against the signature set is the main drawback of an intrusion detection system (IDS) that relies solely on the collection of known signatures. As with normal IDS, employing individual signatures has a single entry for each of their entries, therefore it may have hundreds or even thousands of these entries. The signature-based intrusion detection system uses a signature database of past assaults to detect and identify new ones. It is interesting to note that, although this approach proved successful in obtaining low false alert rates, it is completely useless against zero-day attacks [10]. In order to integrate an anomaly-based intrusion detection system (IDS) for wired, wireless, and cloud networks, Maid claims that theoretical and practical enhancements of behavioral profiling algorithms and statistical approach models were carried out. This solution uses event logs, large transfer files and transfer times, TCP and UDP addresses, CPU usage, weak and synthetic data, internet protocol, and MAC address as a parameter, and you can use statistical methods to create a real-time efficiency model to identify risks. Figure 1: A screen grab of the current network obtained from Resource Monitor's Network tab. For additional analysis, the characteristics listed in Figure 1 will be consulted.

2 Methodology

Identifying unknown attacks in a cloud network using a combination of signature and anomaly-based intrusion detection systems in an artificial intelligence-based multi-layered approach is one part of the objective of this paper. Therefore, the proposed work has been divided into multiple layers.

In the first (I) layer, attribute information is collected and stored in the database tool. Then, the attributes and signatures are verified to determine whether the user is authorized, based on the requirements of the signature-based intrusion detection system. If the user is authorized, the current layer proceeds to the next layer based on the user's request. The second (II) layer fulfills the user's request by the server or network system. The process details are also stored in the database. According to the literature, a large number of entries need to be stored dynamically in the database to increase time efficiency in the cloud. Therefore, a big data tool like SQL Server-based PHPMYADMIN has been utilized. After completing the process, an acknowledgment of the process is sent to the user and administrator, marking the third (III) layer of the proposed system. Figure 2 describes the contribution of the proposed multilayer hybrid IDS and its architecture. Continuing from the first (I) layer, if the user is not authenticated, the current layer proceeds to the second (II) layer based on the user's request. In the second layer, three dynamic keys are generated, one of which is used by the user to enter the third (III) layer.

Additionally, another two dynamic keys are generated by the system. One dynamic key is used by the administrator of the server to grant the user access to files, which is confirmed by the file's author. Upon receiving confirmation from the author, another dynamic key is used. Based on the author's rights, the administrator will provide authentication to the unknown user for

accessing the file. The author of the file sets limits for the user's access, such as read-only, read-and-write, or delete permissions. All these processes are stored as multiple records. Based on these entries, the user can proceed to the next layer. If the user does not receive authentication, they may be considered an attacker.

2.1 Proposed Algorithm: AI-based Multilayer Hybrid IDS (AIML-HyIDS)

- *Step 1: Logs entropy (or Information gain) from Server*
- *Step 2: Identify the Process and respective PID (Process Identification Number)*
- *Step 3: Identify the IP (Internet Protocol) Address for each Process using PID.*
- *Step 4: Identify the TCP/ UDP transformation Process*
- *Step 5: Identify the Active Time and Response time for each process.*
- *Step 6: Identify the Data Packet transformation and Data Packet Loss*
- *Step 7: Trace the IP Address and its behavior of Transformation*
- *Step 7a: Signature attributes verified in the server*
- *Step 8: Classify the Authorized and Unauthorized Transformation*
- *Step 8a: if the user is an unauthorized, three different dynamic keys are generated.*
- *Step 8b: One dynamic key sent to the user, the next dynamic key is stored as a signature and the last one is shared with the administrator.*
- *Step 8c: The administrators' dynamic key is used by the administrator of the server to grant the user access to files, which is confirmed by the file's author. Upon receiving confirmation from the author, another dynamic key is used.*
- *Step 8d: Based on the author's rights, the administrator will provide authentication to the unknown user for accessing the file.*
- *Step 9: Make the Prevention from the Unauthorized Transformation by the administrator.*

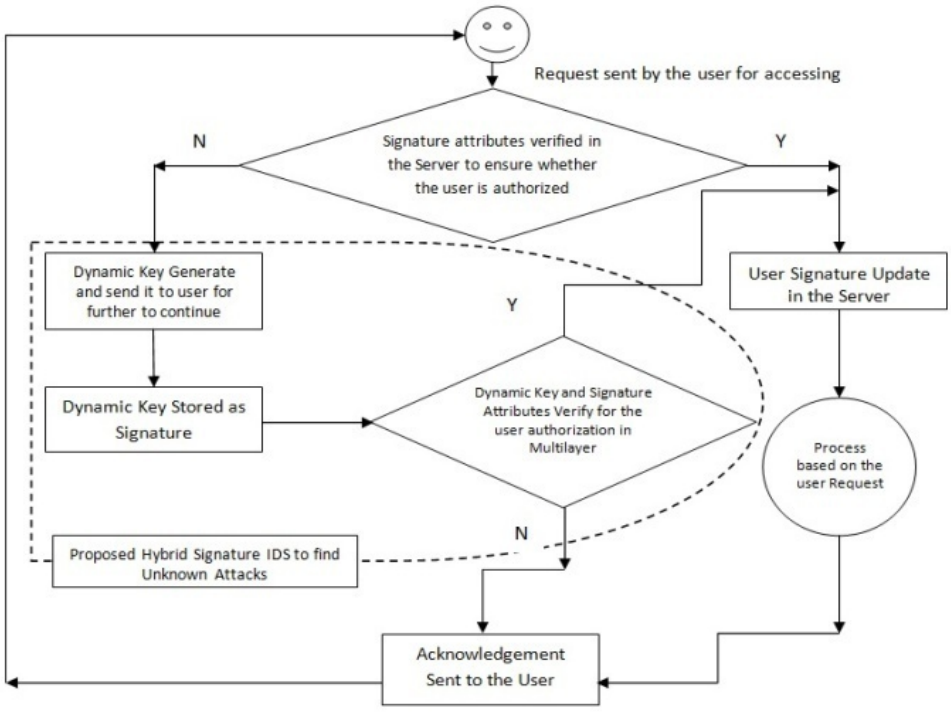

Fig 2. Architecture of the proposed model

2.2 Dynamic Key Generation

A dynamic key is a combination of alphanumeric codes used to obtain user authentication from an administrator or server to access protected files. Dynamic keys are classified into symmetric keys and asymmetric keys. Generally, keys are generated

using two basic techniques: (i) a mathematical approach and (ii) an entry time sequence approach. Symmetric keys can only be used once by a user and are also utilized as session keys. They must be used for a specific period of time, a method known as session keying. Asymmetric keys, on the other hand, can be used as distribution keys and session keys, meaning they are shared by one or more users. To achieve a similar level of security, the asymmetric key size must be at least 10 times larger than the symmetric cryptographic key size[12]. A key can be used only once or multiple times within a timeline. A distributed mathematical approach was used to achieve the research objectives. The mathematical dynamic key order is represented as follows

$$n \in N,\ n \geq 1,\ \{DyKi\} = \{DyK1, DyK2 \ldots . DyKn\} \tag{1}$$

Where n is the number of dynamic keys in the sequence and {DyKi} is a sequence of dynamic keys.

$$\{DyKi\},\ 1 \leq i \leq n\ dynamic\ keys \tag{2}$$

The condition underlying the dynamic generation scheme can be explained in mathematics as: for every algorithm A, the highest probability that A can guess correctly the current dynamic key DyKm from the previous dynamic keys DyKi is, with s being the bits length of dynamic key DyKm.

$$m \in N,\ 1 \leq i \leq m,\ Prob(A(\{DyKi\}) = DyKm) \leq 1/2s \tag{3}$$

This scheme produces a sequence of dynamic keys, which can be unlimited in size, and the number of keys may be infinite.

The sequence must have the following characteristics:

(i) The sequence of keys must be unique for both sender and receiver.

(ii) Previous dynamic keys should not compromise the security of current and future keys in the sequence.

Generate a sequence of dynamic keys - this step is the same as Step 4 in the initial dynamic key generation scheme. The new seed key SdK^' and the new temporary keys TempK1^'…..TempKm' are used to calculate the new dynamic key sequence

$$DyK1' \ldots . . DyKm' \tag{4}$$

$$\begin{aligned} DyK1' &= f(SdK', TempK1', TempK2', \ldots . ., TempK'\ m-2, TempK'\ m-1, TempK'\ m) \\ DyK2' &= f(SdK', TempK2', TempK2', \ldots . ., TempK'\ m-1, TempK'\ m, DyK1') \\ DyK3' &= f(S[dK]', TempK3', TempK4', \ldots . ., TempK'\ m, DyK'\ 1, D[yK]'\ 2) \\ \ldots . . & \end{aligned}$$

$$DyKn' = f(S[dK]', D[yK]'\ n-m, \ldots . ., DyK'\ n-3, D[yK]'\ n-2, DyK'\ n-1) \tag{5}$$

The secure lifetime for a dynamic key is calculated as follows. It is assumed that in a unit of time, an adversary can perform x' trials to break a dynamic key. x's trials and the probability of guessing correctly the dynamic key sequence is reduced to be

$$Prob(DyKi) = 1/(2s - x't) \tag{6}$$

The dynamic key theory has drawbacks regarding synchronization, particularly in symmetric encryption where the dynamic keys used between the sender and receiver must match. Synchronization issues can arise due to various reasons:

- **Malicious attacks from opponents or connectivity issues:** An attacker could impersonate the sender and send a message encrypted with a random key, confusing the recipient. Additionally, adversaries may launch man-in-the-middle attacks to disrupt or intercept communications and alter message content. Connectivity issues, common in wireless networks, can also disrupt communication.
- **Broken clients or stolen devices:** Issues with client devices can lead to synchronization problems.
- **Interruption of the dynamic key sequence by attackers:** Attackers may interfere with the dynamic key sequence, causing synchronization issues.

To address synchronization problems caused by adversarial attacks, adding authentication to communications can be beneficial. By restricting dynamic key changes within authenticated communications, messages from masked senders can be detected and ignored.

2.3 Performance Evaluation

The C5.0 decision tree classifier was used to evaluate the performance of the Signature-based Intrusion Detection System (SIDS), while the support Vector Machine was utilized to evaluate the performance of the Anomaly-based Intrusion Detection System. The proposed Hybrid Intrusion Detection System, a combination of Signature and Anomaly-based Intrusion Detection Systems, had its performance evaluated using both C5.0 and one-class SVM classifiers. For evaluation metrics, two classes, namely predicted and actual class, were used. Confusion Matrix measurements were conducted to assess the performance between the attacks. Confusion Matrix measurement as in Table 1.

Table 1. Evaluation Confusion Matrix Classes

Actual Class	Predicted Class	
	Malware	**Normal**
Normal	False Positive (FP)	True Negative (TN)
Malware	True Positive (TP)	False Negative (FN)

- Step 1: True Positive Rate (TPR) has to be found for measuring the quantitative relationship. It is also called as Detection Rate (DR).

$$True\ Positive\ Rate\ (TPR) = TP/(TP+FN) \tag{7}$$

- Step 2: False Positive Rate (FPR) has to be found for measuring the quantitative relationship between normal cases that are detected as attacks.

$$False\ Positive\ Rate\ (FPR) = FP/(FP+TN) \tag{8}$$

- Step 3: False Negative Rate (FNR) has to find IDS could not classify the threats and classified as Normal.

$$False\ Negative\ Rate\ (FNR) = FN/(FN+TP) \tag{9}$$

- Step 4: The accuracy of the IDS is classifying normal and Intrusion attacks. It is also called as Classification Rate (CR).

$$Accuracy\ (or)\ Classification\ Rate = \ (TP+TN)/\ (TP+TN+FP+FN) \tag{10}$$

- Step 5: Precision (P) has to be identified by using the percentage of total true positive.

$$Precision = TP/(TP+FP)*100\% \tag{11}$$

- Step 6: Recall (R) has to identify which refers to the total percentage of total relevant results correctly classified.

$$Recall = TP/(TP+FN)*100\% \tag{12}$$

- Step 7: F-measure is the mean of the precision and Recall.

$$F-measure = \ (2*R*P)/(R+P) \tag{13}$$

3 Results and Discussion

When assessing this approach, it can be helpful to keep in mind that its main goal is to detect every known attack, and its efficacy is approximately 98%. In reference to the last one, the behavioral profiling algorithm experiment was carried out with the supposition that the system's log files produce one thousand entries depending on one thousand four hundred and forty attributes for the client. Five nodes are added to the server for each moving 120-second interval, and the efficiency of the current models has been properly compared to the existing models' efficiency using the selected attributes. The following table displays qualitative metric evaluation data from existing models. Figure 3 shows the original time series representation of the dataset from the existing model's log file and synthetic weak data.

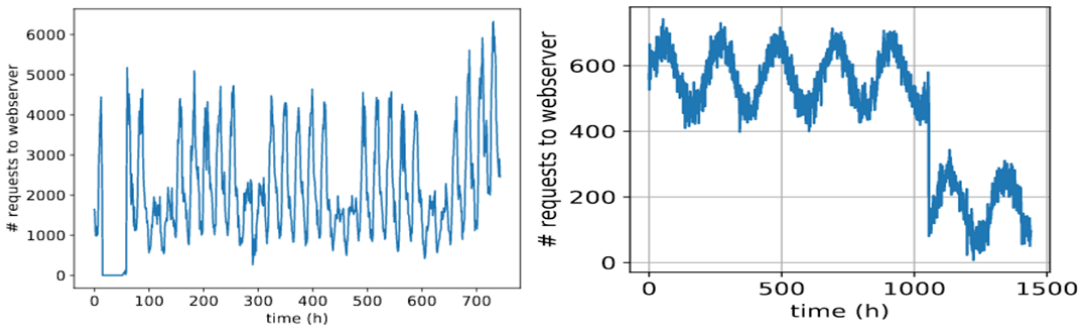

Fig 3. The existing model's log file and synthetic weak data

Table 2 describes the existing model evaluation metrics such as log requests, CPU Usage, and Weak and Synthetic Data.

Table 2. Existing model evaluation metrics

No of Nodes	Logs requests in Web Server	CPU Usage (%)	Weak Data	Synthetic Data
5	1286	172	301	985
10	2579	198	538	2041
15	4048	254	798	3250
20	6580	272	1763	4817
25	8781	287	1992	6789
30	10521	346	2089	8432
35	12482	380	1640	10842
40	16754	421	1989	14765

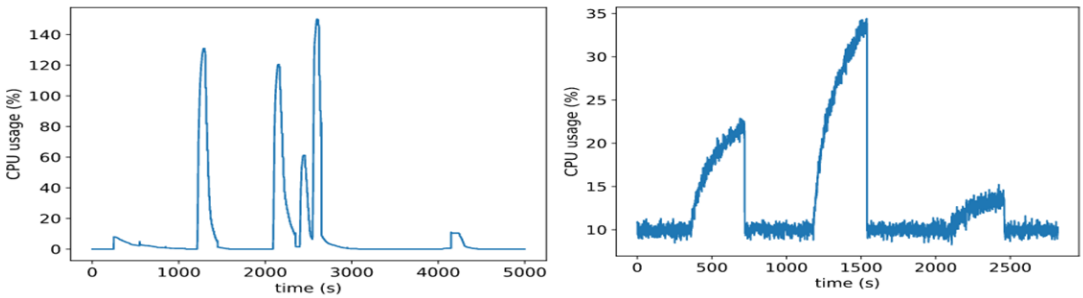

Fig 4. CPU usage in the trace and CPU usage

Table 3 illustrates the qualitative metric evaluation data from the proposed model. Memory and CPU usage were taken into account for analysis.

Table 3. Proposed model evaluation metrics

No of Nodes	Logs requests in Web Server	CPU Usage (%)	Weak Data	Synthetic Data
5	1321	128	122	1199
10	2647	57	178	2469
15	3948	132	320	3628
20	6893	157	492	6401
25	9012	138	581	8431
30	11142	198	648	10497
35	12987	212	706	12281
40	17358	230	912	16446

Figure 4 describes the CPU usage in the trace and CPU usage while various numbers of applications are running on the network. Through this table, it is found that the proposed model achieves above 90% accuracy. NSL-KDD and ADFA benchmark datasets were utilized to evaluate accuracy and performance. Totally 22544 and 82332 data records were gathered from NSL-KDD and ADFA respectively. After data cleaning 22500 and 82300 data records are taken for evaluation. SQL Server-based PHPMYADMIN database and Personal Home Page (PHP-5.0) were employed to create dynamic web pages and enable interactivity. Web services were enabled using Tomcat with PID 8020 and ports 8005 and 8080. The confusion matrix results of the C5.0 Classifier, the Performance of the Support Vector Machine, and the Proposed Hybrid IDS results are presented in Table 4. Performance Evaluation on C5.0 classifier, SVM, and proposed model with NSL-KDD and ADFA dataset are presented in Table 5.

Table 4. C5.0 classifier, Performance of the SVM, Confusion matrix result of the proposed model with NSL-KDD and ADFA dataset

Dataset	NSL-KDD		ADFA	
Class	**Malware**	**Normal**	**Malware**	**Normal**
Confusion matrix results with the use of C5.0 classifier on NSL-KDD and ADFA dataset				
Normal	278	9397	938	36058
Malware	8907	3918	44069	1235
Performance of the Support Vector Machine				
Normal	208	9467	3918	33065
Malware	6754	6071	29769	15548
Confusion matrix results of Proposed Hybrid IDS				
Normal	184	9491	3904	33079
Malware	6773	6052	29753	15564

Table 5. Performance Evaluation on C5.0 classifier, SVM, and proposed model with NSL-KDD and ADFA dataset

Class	NSL-KDD			ADFA		
	TP-Rate	**FP-Rate**	**F Measure**	**TP-Rate**	**FP-Rate**	**F Measure**
Accuracy of C5.0 decision tree on NSL-KDD and ADFA dataset						
Normal	0.970	0.028	0.819	0.974	0.025	0.975
Malware	0.694	0.030	0.805	0.972	0.020	0.976
Accuracy of the One-class Support Vector Machine on NSL-KDD and ADFA dataset						
Normal	0.978	0.473	0.752	0.894	0.343	0.773
Malware	0.527	0.022	0.683	0.657	0.106	0.754
Accuracy of Proposed Hybrid IDS on NSL-KDD and ADFA dataset						
Normal	0.972	0.273	0.833	0.976	0.029	0.971
Malware	0.727	0.028	0.832	0.971	0.024	0.977

4 Conclusion

This study presents a multi-layered artificial intelligence-based method that combines anomaly and signature-based intrusion detection systems (IDS) to detect unexpected attacks targeting cloud networks. Creating a model with the ability to recognize and react to cyber threats in cloud environments was the goal. In order to obtain knowledge about current intrusion detection methods and how they are used in diverse network contexts, we carried out an extensive review of the literature.

With the help of anomaly-based IDS and signature-based IDS, the suggested model can detect recognized threats and unexplained patterns of behavior that might point to novel or never-before-seen attacks. We sought to increase the overall efficacy of intrusion detection in cloud networks by fusing these two methods into a multi-layered framework.

Some of the Literature said that the existing model while using the Hybrid Intrusion detection model can identify unknown attacks with a maximum of 80%, 92%, and 96% accuracy respectively. The NSL-KDD and ADFA benchmark datasets were used in our experiments, and the results showed how well the suggested model performed in terms of accuracy and detection rates. The C5.0 decision tree classifier and Support Vector Machine were employed to assess the efficacy of signature-based and anomaly-based intrusion detection systems, respectively. We also demonstrated the accuracy metrics and confusion matrix findings for the suggested Hybrid IDS on both datasets. The current paper identifies unknown attacks in the cloud network using a combination of signature and anomaly-based intrusion detection systems in an artificial intelligence-based multi-layered approach and it produced above 97% accuracy.

According to the results, the suggested Hybrid IDS outperformed other models in terms of detection performance and accuracy rates. More specifically, our model showed excellent accuracy in identifying both benign and malevolent activity in cloud networks. Additionally, the multi-layered strategy worked well for thwarting different kinds of threats and guaranteeing strong security.

Ultimately, by successfully detecting and reducing cyber threats, the suggested multi-layered method is a viable means of improving cloud network security. Further, model optimization, the incorporation of new machine learning algorithms, and the investigation of cutting-edge technologies like deep learning and the Internet of Things are possible future research avenues that could enhance detection capabilities and fortify network defenses against constantly changing cyber threats.

References

1) Saraniya G. Securing the Network Using Signature Based IDS in Network Intrusion Detection System. *International Scientific Referred Research Journal*. 2019;2(1):99–101. Available from: https://shisrrj.com/paper/SHISRRJ192119.pdf.
2) Bhardwaj A, Al-Turjman F, Kumar M, Stephan T, Mostarda L. Capturing-The-Invisible (CTI): Behavior-Based Attacks Recognition in IoT-Oriented Industrial Control System. *IEEE Access Special Section on Edge Intelligent for Internet of Things*. 2020;8:104956–104966. Available from: https://doi.org/10.1109/ACCESS.2020.2998983.
3) Snehi J, Bhandari A, Vidhubaggan, Snehi M, Ritu. Diverse Methods for Signature based Intrusion Detection Schemes Adopted". *International Journal of Recent Technology and Engineering*. 2020;9(2):44–49. Available from: https://doi.org/10.35940/ijrte.A2791.079220.
4) Cyril OO, Elmissaoui T, Okoronkwo MC, Uchechi IM, Chikodili H, Ugwuishiwu OB, et al. Signature based Network Intrusion Detection System using Feature Selection on Android. *International Journal of Advanced Computer Science and Applications*. 2020;11(6):551–558. Available from: https://doi.org/10.14569/IJACSA.2020.0110667.
5) Einy S, Oz C, Navaei YD. The Anomaly- and Signature-Based IDS for Network Security Using Hybrid Inference Systems. *Mathematical Problems in Engineering*. 2021;2021:1–10. Available from: https://doi.org/10.1155/2021/6639714.
6) Sommestad T, Holm H, Steinvall D. Variables influencing the effiectiveness of signature-based network intrusion detection systems. *Information Security Journal: A Global Perspective*. 2022;31(6):711–728. Available from: https://doi.org/10.1080/19393555.2021.1975853.
7) Markevych M, Dawson M. A Review of Enhancing Intrusion Detection Systems for Cybersecurity using Artificial Intelligence (AI). *International Conference Knowledge-Based Organization*. 2023;29(3):30–37. Available from: https://doi.org/10.2478/kbo-2023-0072.
8) Gaharwal R, Kumar P. Detection techniques for Intrusion Detection System (IDS). *Academic Journal of Information Security*. 2019;1(1):16–20. Available from: https://www.xournals.com/assets/publications//AJIS_V01_I01_P16-20_01-2019.pdf.
9) Thankappan M, Rifa-Pous H, Garrigues C. A Signature Based Wireless Intrusion Detection System Framework for Multi-Channel Man-in-the-Middle Attacks Against Protected Wi-Fi Networks. *IEEE Access*. 2024;12:23096–23121. Available from: https://doi.org/10.1109/ACCESS.2024.3362803.
10) Tang TA, Mclernon D, Lotfimhamdi, and SARZ. Intrusion Detection in SDN-based Networks: Deep Recurrent Neural Network Approach", Advanced Sciences and Technologies for Security Applications. Cham, Switzerland. Springer. 2019. Available from: https://doi.org/10.1007/978-3-030-13057-2_8.
11) Kawaguchi H, Nakatani Y, Okada S. IDPS Signature Classification Based on Active Learning With Partial Supervision From Network Security Experts. *IEEE Access*. 2022;10:105713–105725. Available from: https://doi.org/10.1109/ACCESS.2022.3211651.
12) Ya S, Hilgurt AM, Davydenko TV, Matovka MP, Prygara. Tools for Analyzing Signature-Based Hardware Solutions for Cyber Security Systems". *Journal of Cyber Security and Mobility*. 2023;12(3):339–366. Available from: https://doi.org/10.1155/2021/6639714.
13) Diaz-Verdejo J, Munoz-Calle J, Alonso AE, Alonso RE, Madinabeitia G. On the Detection Capabilities of Signature-Based Intrusion Detection Systems in the Context of Web Attacks. *Applied Sciences*. 2022;12(852):1–16. Available from: https://doi.org/10.3390/app12020852.
14) Mehta V, Pal P. Internet Security: Intrusion Detection Systems (IDS). *Journal of Emerging Technologies and Innovative Research*. 2023;10(1):a751–a756. Available from: https://www.jetir.org/papers/JETIR2301094.pdf.