IMPROVED INTRUSION DETECTION SYSTEM FOR CLOUD COMPUTING: A SURVEY

B. Sankaraiah
Assistant Professor, Department of Computer Science & Engineering, Malla Reddy (MR) deemed to be University, Hyderabad. Email id.: Shankar61186@gmail.com
Vemula Nikitha
Assistant Professor, Department of Computer Science & Engineering, Malla Reddy (MR) deemed to be University, Hyderabad. Email id.: nikitha479@gmail.com
Syed Abdul Haq
Assistant Professor, Department of Computer Science & Engineering, Malla Reddy (MR) deemed to be University, Hyderabad. Email id.: abdulhaq007@gmail.com
Dr. Syed Umar
Professor, Department of Computer Science & Engineering, Malla Reddy (MR) deemed to be University, Hyderabad. Email id.: syedumar@mrec.ac.in

Abstract—Cloud computing has revolutionized the technology landscape with its scalability and cost efficiency. However, it has also introduced unique security challenges. System Aided Design (SAD) has emerged as a vital tool in addressing these issues by enhancing the classification of security threats specific to the cloud environment. While cloud computing does offer flexibility and economic advantages, the extensive sensitive data involved raise concerns about data security and privacy. Intrusion Detection Systems (IDSs) are pivotal for cloud security but face challenges due to the dynamic nature of the cloud. This research work focuses on developing a cloud-based IDS using neuro-swarm intelligence techniques to efficiently analyze and classify network traffic, adapting seamlessly to the dynamic cloud landscape. This approach promises to be a robust solution for safeguarding data and ensuring secure cloud operations. A comprehensive evaluation of an Intrusion Detection System (IDS) that utilizes G-ABC and DNN techniques has been performed under this research work. Moreover, this research work goes beyond the well-detected DoS attacks to assess the IDS's performance in identifying U2R, R2L, and Probes attacks using both the NSL KDD and UNSW NB15 datasets. The analysis includes precision, recall, F-measure, and accuracy metrics, highlighting the IDS's potential to enhance intrusion detection across various attack categories.

INDEX - Cloud computing, Intrusion Detection System (IDS), WSN, Dataset, Attacks, Algorithm, etc.

I. INTRODUCTION

Cloud Computing (CC) has always been an area of interest for the researchers. When it was thought of cloud in the early years starting from 2008, cloud was defined as an execution unit with fast execution capabilities [1]. Later on, with the evolution of cloud and application architecture, cloud started to provides services that are related to infrastructure as well. The cloud has three layers of computation namely Infrastructure as Service (IaaS), Platform as Service (PaaS) and Software as Service (SaaS) [2]. The IaaS involves all the hardware oriented operations that contains the physical aspects of the cloud. As for example, IaaS will have super end processors, task scheduling units, the negotiator with the client to decide Service Level Agreements (SLAs). Any application to be executed on any infrastructure, requires a platform in terms of operating system and hence PaaS service must be integrated to provide SaaS. Due to increasing number of users on cloud networks, there are several types of security aspects that a cloud is concerned like maintaining the SLA first of all, managing the energy efficacy in the service provisioning and preventing the overload on the execution elements of the cloud like a Physical Machine (PM). The security framework at any computation platform can be easily segregated into two aspects. The first aspect is user authentication and provisioning of the access control architecture popularity known as Role Based Access Control (RBAC) [3]. The cloud needs to perform RBAC process to make sure that the correct information reaches to the correct person of correct level. However, the first aspect is quite interesting to get focus and researchers from around the world has contributed significantly for the same, but, the proposed work is focused on the second aspect of the security. The second aspect refers to network level security in which the cloud server gets anonymous number of requests per second. Due to advancements in data science, the fruit of knowledge has also produced poisons to the computation models of cloud and they are referred as security attack in this research draft. Due to high volume of users, it is hard to identify and mark the security attack manually and that even when there are varieties in security attacks. If a cloud fails to identify the risk in the early stage, the consequences could be massive in terms of losses. The intruder may breach into secret accounts and can reveal a lot of information or for the time being the intruder may also misuse it against a specific group of persona. In such a scenario, early detection of security attack or threat can only be done using System Aided Design (SAD). Any SAD architecture consists of two portions namely training and classification. The classification score defines the preciseness of the training. The training aspect involves the data selection suitable to its category in terms of feature and feature vector. This research draft illustrates a modified selection algorithm and improves the overall classification rate for variety of attacks [4].

Cloud Computing

Cloud computing is a platform in which virtualized resources are made available as a pay-peruse service, similar to power is distributed in an electrical grid [5]. Websites and web-based applications were set up on a single system prior to this arrangement. The resources were constrained together as a virtual computer with the development of this technology. The benefits of cloud computing for businesses include the ability to connect and collaborate globally without the need to build up additional infrastructure, such as servers, datacenters, and other facilities. The environment can support a large number of users because it is scalable. The key benefits of switching to this computer paradigm include lower costs, less reliance on staff, resilient scalability, and others [6]. Social networking and other forms of interactive technology are included in cloud computing, although for the most part, cloud computing refers to the utilization of internet software applications, data management, and computational power. Without investing in additional hardware, employing more employees, or obtaining software licences, cloud computing allows for the dynamic easing of congestion or addition of capabilities. It increases information technology's (IT) potential. Over the past several years, cloud computing has evolved from a potential business idea to one of the IT sectors with the quickest rate of growth. But as more and more information about individuals and companies is kept on cloud servers, concerns over the environment's security are beginning to surface. [7].

Aspects of Cloud Computing

CC has revolutionised information processing by providing a technology platform that is affordable, efficient, and scalable. From an administrative standpoint, cloud computing offers greater storage and processing capacity at a lower cost. According to a Market Research Media report, the world's cloud computing 30 percent compound annual growth rate (CAGR) is anticipated for the market, which is projected to reach $270 billion in 2020 [8]. Though, the Cloud-based crimes and assaults against clouds and their users are more challenging to forestall and look into because of aspects that make cloud computing so strong [9].

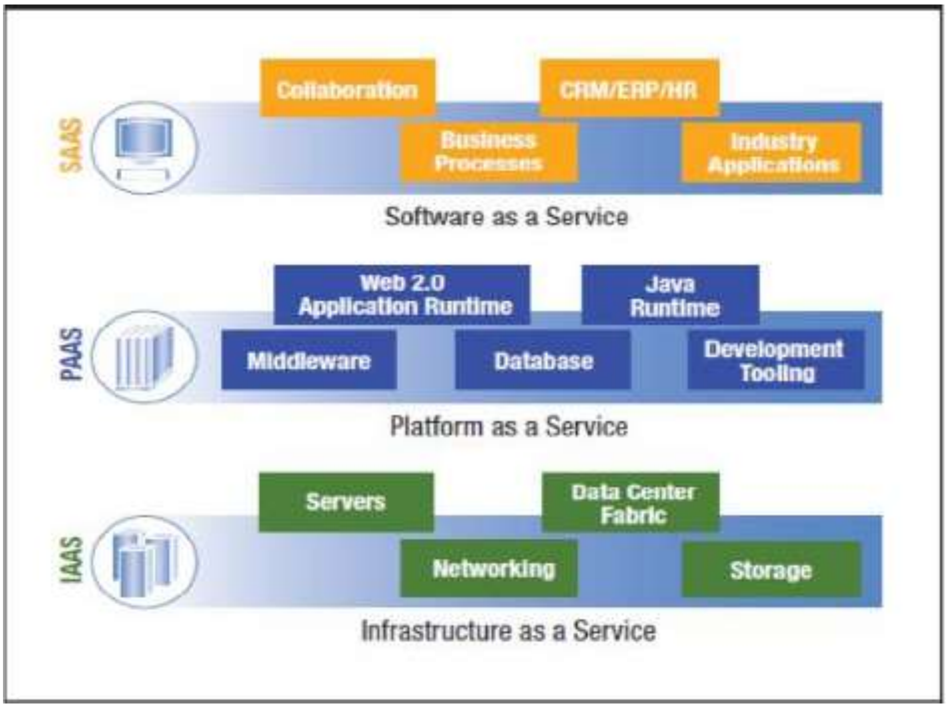

Figure 1: Cloud Computing Service Delivery Model [10]

Computational resources are offered as services via the Internet using cloud computing, an ondemand, pay-per-use computer architecture. With the use of this technology, clients may obtain software or hardware resources that are managed and hosted by a Cloud Service Provider (CSP) from a distance and receive a cheaper, preconfigured infrastructure. The three service models provided by cloud computing are Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS), as shown in Figure 1.

Security Attacks in Cloud

Although the CC paradigm is not very big, there are many security breaches that are made against different cloud deployment methodologies, posing a substantial risk to users of the cloud. [10]. For instance, a number of attacks such as inundation, wrapper, malicious insertion, side passage, and cryptography man-in-the-middle techniques, and authentication attacks against
cloud computing are possible [11].

Table 1: Attacks on the cloud component

Attacks	Protocol vulnerability exploitation	Spoofing	Incurring high load	Gain access to hypervisor
Cloud Internal DoS	Yes	No	Yes	No
Neighbour attacks	No	No	Yes	No
Mimicking DoS	No	No	No	Yes
Application DoS	Yes	No	No	No
Energyoriented DoS	No	No	Yes	No
VM escape	No	No	No	Yes

DoS and DDoS attack

A denial-of-service (DoS) attack is any event or malicious action that lessens or prevents a cloud's capacity to provide the services and functionalities that users expect [12]. Circulated version of Distributed DoS (DDoS) attacks is referred to as DoS attacks. It uses many network hosts to do more damage damaging consequences for its sufferer. A DoS attack is one that

targets a resource or service in the cloud with the intention of temporarily preventing it from offering its regular services.

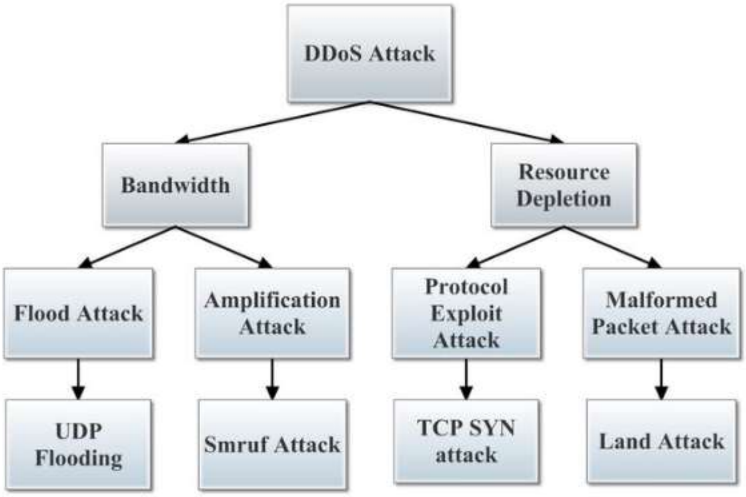

Figure 2: Classification of DoS attacks

DoS attacks frequently target the connectivity or capacity of computer networks, which jeopardises the accessibility of cloud services and resources. Generally, DoS attacks occur due to bandwidth restriction, problem in connectivity, exhausting of resources, limitation of exploitation, disruption in processes, corrupted data, and due to physical disruption [13]. The classification of DoS attacks is illustrated in Figure 1.2. A distributed denial of service (DDoS) attack involves the use of many hacked computers to overload a target system with traffic, rendering it inaccessible to its intended users. In cloud computing, DDOS attacks can be classified into several types, based on the nature of the attack and the way it is carried out. Some common types of DDOS attacks in cloud computing are:

Volume-based attacks: In order to overrun the target system and prevent it from being used by its intended users, these attacks try to overload it with a lot of traffic, such as HTTP requests or network packets.

Protocol-based attacks: By taking advantage of flaws in the TCP/IP protocol stack and other communication protocols utilised by the target system, these attacks make the system inaccessible and clogged.

Intrusion Detection System (IDS)

Intrusion detection is usually referred to the technology and the software applications that monitor the network activities and detect security breaches in terms of malicious activities. Soon after Dorothy Denning work on the initial IDS model presented at SRI international [14], a number of intrusion detection works were put forth to address the challenges of research industry. The generalized architecture of the IDS system shown in figure 3 included the following components:

- Sensors that gather and collect the data from the system to be monitored.
- Detector which is also known as intrusion detection engine which perform analysis of malicious activities on the data collected from the sensor.
- Knowledgebase is the database that act as a repository for the pre-processed version of the collected information using sensors. It is also annotated for the attack signature, profiles, etc. to help security experts.
- Configuration device is used to share information regarding the current state of the IDS.

- Response Component is the last component of the system that initiates action as and when an intrusion is detected by the system. The generated response can be customized and may or may not involve human intervention.

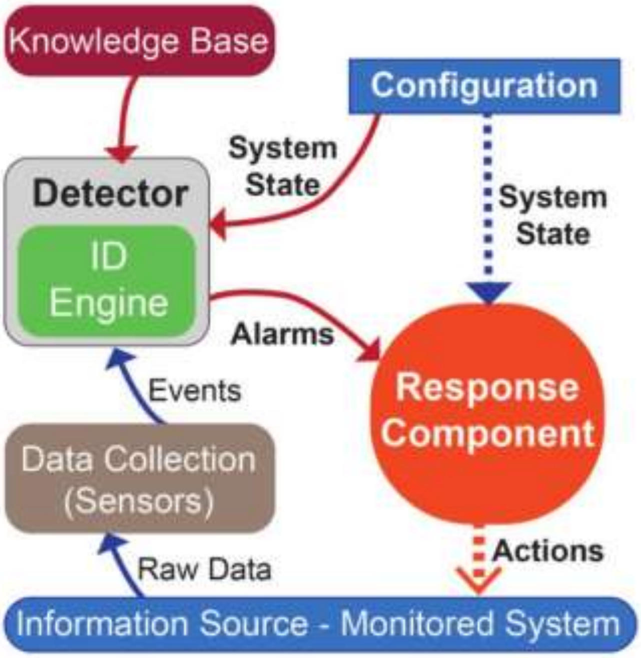

Figure 3: IDS Architecture

These intrusion detection tools or the intrusion detection systems (IDS) are aimed at identifying the security threats in real time scenario and are broadly classified as follows.

Network based IDS (NIDS)

This type of IDS analyses the network packets to identify the suspicious patterns that looks deviated from the usual pattern. As soon as the malicious activity is detected, it generates a predefined action to mitigate the potential threat.

Host based IDS (HIDS)

This type of IDS is installed on an individual computer system and monitors the activity of the specific host computer system. It analyses the behaviour of various processes, user activity and files for the host system to detect any abnormal activity or unauthorized access attempts to the system files. The IDS forms one of the critical component of the cyber security that helps in identifying any security breaches, cyber-attacks, etc.

Characteristics of IDS

Effective IDS is an essential part of present day security strategies that help organizations to detect and monitor the security breaches and. attacks. From the security point of view prediction efficiency, time balanced performance and fault or anomaly detection are some of the major characteristics of an IDS in addition to the following.

- Detect anomaly based on monitoring normal network patterns.
- Timely generate warning alerts.
- Ability for real-time processing and detection.
- Accurately differentiate different anomaly patters of different attacks.
- IDS should be scalable to accommodate large and complex processing.
- It should have low false positive rate.
- It should be adaptive to learn to detect evolving threats and attacks.

II. LITERATURE REVIEW

The utility computing is possible with cloud computing that includes monitoring tools, storage tools, analytics tools, visualisation platforms, and client delivery. Due to cloud computing's subscription-based pricing model, organisations and individuals will be able to have on-demand access to a wide variety of useful apps from any location. Sharing information is key to cloud computing, which is now widely used for the transfer of sensitive information worldwide. Data stored in the cloud is vulnerable to security breaches because all users have access to it [15]. There are numerous hackers trying to breach security and use the cloud's facilities. The security breach is a serious issue that could disrupt cloud services. In order to prevent users from accessing data stored in the cloud, hackers deploy a variety of techniques.

Jaber and Rehman (2020) presented a novel IDS that integrated the fuzzy c means clustering (FCM) approach including SVM with the aim to enhance the accuracy of presented approach in clud computing envirornmet. For simulation purpose, NSL-KDD dataset has been considered. With the aim to analyse the performance of proposed work, the results found using this novel hybrid approach i.e. FCM-SVM indicated that this scheme can detect the anomalies from network with enhanced detection accuracy including lower false alarm rate [16].

Islabudeen and Devi (2020) proposed an intelligent framework to mitigate attacks in MANET by using the ML approach for detecting and preventing intrusion systems (SA-IDPS). Initially, mobile users used the one-way hash chain function to register with trusted authorities. The implementation was carried out with the help of a type-2 fuzzy controller, which compiled data
from the package header. The extraction of the optimal set of functions for classification purposes was done using mutual knowledge in the future extraction. User to root (U2R), Remote to local (R2L), anomaly, DoS, and Probe are five groups of packets that are classified using a bootstrapped positive algorithm for tree construction with ANN, if the attack is frequent or rare [17].
Velliangiri et al. (2021) addressed the security of cloud information, specifically focusing on mitigating Distributed Denial of Service (DDoS) attacks. The Taylor-Elephant Herd Optimisation based Deep Belief Network (TEHO-DBN) is a deep learning-based classifier that they introduced. The study involved the collection and grouping of user service requests as log
information. To enhance the classification process and reduce training time, relevant features were selected from the log file using the Bhattacharya distance measure. The Deep Belief Network (DBN) was trained for DDoS attack detection using the TEHO-DBN method, which was created by combining the Taylor series with Elephant Herd Optimisation (EHO). The suggested TEHO-based DBN classifier showed improved performance, reaching a maximum accuracy of 0.830, according to simulation findings [18].
Eren et al. (2023) successfully used both machine learning and deep learning approaches to carry out a thorough attack detection procedure on the UNSW-NB15 and NSL-KDD datasets. The study showed that by integrating these technologies, accurate attack detection and classification could be accomplished. Accuracy values of 98.6% and 98.3% were obtained for
two-class and multi-class classification in the UNSW-NB15 dataset, respectively. Similarly, the NSL-KDD dataset yielded accuracy rates of 97.8% for two-class and 93.4% for multi-class classification. These results underscore the effectiveness of machine learning algorithms as a viable solution for intrusion detection systems [19].

III. METHODOLOGY

In the light of the detailed literature survey, four classifiers namely, Deep Neural Network (DNN) with multiple layers, Back Propagation Neural Networks (BPNN) Naïve Bayes (NB) and Support Vector Machine (SVM) have been predominately employed for similar task. Therefore, a comparative analysis of these classifiers is performed in this chapter to find their effectiveness to defend each attack used in the study.
As the algorithm aims to design SAD based architecture they require a training and a classification mechanism and hence the objective that has been framed is to analyse the data security based on the

classifiers. To achieve this objective, based on the literature, four algorithms for training and classification have been selected, namely Deep Neural Networks (DNN), Back Propagation Neural Network(BPNN), Support Vector Machine (SVM) and Naïve Bayes (NB). All of these four algorithms have different architecture of training and the proposed work wanted to conduct a survey over the classification accuracy of the classifiers without any alteration in the dataset [20-22].

Classification Algorithms

As briefed earlier that 4 training and classification algorithms have been considered namely DNN, BPNN, SVM and Naïve Bayes, this section briefly introduced considered classifiers as follows.

Naïve Bayes

The decision tree is one of the most widely used machine learning methods for intrusion detection. A decision tree is a tree-like model that divides the feature space into regions recursively in order to generate predictions. At each node of the tree, a feature is selected and used to split the data into two or more subsets. The process continues until the data in each subset can be confidently classified.

The decision tree can be trained using a dataset of normal and intrusions connections. For example, Let X be the feature matrix, with each column denoting a feature and each row denoting a network link. Let y be the label vector, where yi = 0 if the i-th connection is normal and yi = 1 if the i-th connection is an intrusion.

Naïve Bayes are a popular machine learning technique used in intrusion detection systems (IDSs) for cloud computing. The basic idea behind decision trees as shown in Figure 4, is to use a tree-based representation to model the relationships between various security-related features and the likelihood of an intrusion. The data is recursively divided into smaller subsets according to the feature values to create the Bayes model, which is then used until a set of stopping conditions is satisfied.

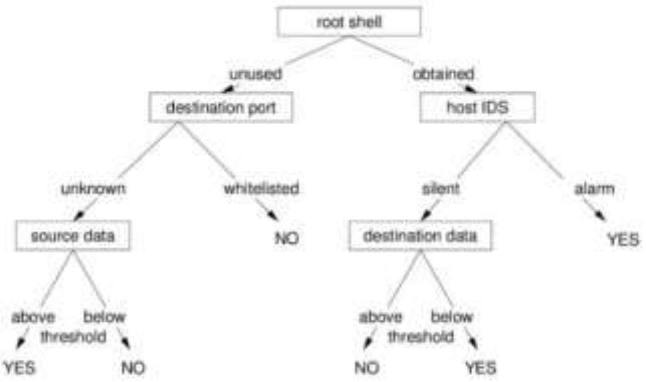

Figure 4: Decision Tree sample

Support Vector Machine

The Support Vector Machine (SVM), a widely adopted supervised learning technique, has proven to be a highly effective solution for addressing classification and regression challenges in various domains, including the field of fetal well-being monitoring. While much of the earlier research efforts were centred on enhancing SVM learning algorithms, the current focus has shifted towards identifying more efficient kernels to further enhance accuracy [22]. Traditional kernels such as Linear, Gaussian, and Polynomial, while useful, may not fully exploit the nuances of specific datasets. As a result, the research community is now actively exploring novel kernel functions that can be applied in contexts like multimedia and signal processing. Kernels play a vital role in determining how well an SVM performs and offer a more streamlined approach compared to the complex methods employed in deep learning. These kernels are essentially mathematical functions designed to take non-linearly separable data as input and convert it into linearly separable data within a higher-dimensional space. In essence, a kernel function calculates the inner product between two data points within an appropriate feature space, creating a measure of similarity with minimal computational overhead, even in instances involving exceedingly high-dimensional data.

IV. CONCLUSION

This section presents a comprehensive evaluation of an Intrusion Detection System (IDS) leveraging the various techniques. The study goes beyond the already well-detected DoS attacks and assesses the IDS's performance in identifying attacks using datasets. Precise analyses of precision, recall, F-measure, and accuracy metrics are provided. The results indicate that the IDS exhibits promising capabilities in enhancing intrusion detection rates across various attack categories. By comparing its performance with established studies, author highlighted its potential to bolster network security by extending effective detection beyond DoS attacks. This research contributes valuable insights into the ongoing efforts to fortify network defenses against an evolving landscape of threats.

REFERENCES

[1] Naveen Sai Bommina, Uppu Lokesh, Nandipati Sai Akash, Dr. Hussain Syed, Dr. Syed Umar, "Optimizing AI-Driven Security Protocols in IoT Networks Using Metaheuristic Algorithms", International Journal of Intelligent Systems and Applications in Engineering, IJISAE, 2024, 12(23s), 3339–3347.

[2] Naveen Sai Bommina, Nandipati Sai Akash, Uppu Lokesh, Dr. Hussain Syed, Dr. Syed Umar, "A Hybrid Optimization Framework for Enhancing IoT Security via AI-based Anomaly Detection", International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169 Volume: 11 Issue: 3.

[3] Nandipati Sai Akash, Uppu Lokesh, Naveen Sai Bommina, Hussain Syed, Syed Umar, "Swarm Intelligence-Based Hyperparameter Optimization for AI-Powered IoT Threat Detection", International Journal of Intelligent Systems and Applications in Engineering, (2024), 12(17s), 941.

[4] Uppu Lokesh, Naveen Sai Bommina, Nandipati Sai Akash, Dr. Hussain Syed, Dr. Syed Umar, "Designing Energy-Efficient and Secure IoT Architectures Using Evolutionary Optimization Algorithms", International Journal of Applied Engineering & Technology, Vol. 4 No.2, September, 2022.

[5] Divya Rohatgi, Dr. Tulika Pandey, "Regression Test Selection Framework for Web Services", INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 9, ISSUE 03, MARCH 2020.

[6] K Sankar, Divya Rohatgi, S Balakrishna Reddy, "COX Regressive Winsorized Correlated Convolutional Deep Belief Boltzmann Network for Covid-19 Prediction with Big Data", Grenze International Journal of Engineering & Technology (GIJET), Grenze ID: 01.GIJET.9.1.547, © Grenze Scientific Society, 2023.

[7] Thakre N, Nimma D, Turukmane AV, Singh AK, Rohatgi D, Bangaru B (2024) Dynamic path planning for autonomous robots in forest fire scenarios using hybrid deep reinforcement learning and particle swarm optimization. Int J Adv Comput Sci Appl 15(9).

[8] Ahmad, Z., Khan, A. S., Aqeel, S., Julaihi, A. A., Tarmizi, S., Annuar, N., & Habeeb, M. S. (2022, May). S-ADS: spectrogram image-based anomaly detection system for IoT networks. In 2022 Applied Informatics International Conference (AiIC) (pp. 105-110). IEEE.

[9] Habeeb, M. S., & Babu, T. R. (2024, October). Enhancing IoT Security Through Advanced Feature Selection and Deep Learning. In International Conference on Computing and Communication Networks (pp. 37-49). Singapore: Springer Nature Singapore.

[10] Uppu Lokesh , Naveen Sai Bommina , Nandipati Sai Akash , Dr. Hussain Syed , Dr. Syed Umar. (2021). Deep Reinforcement Learning with Genetic Algorithm Tuning for Intrusion Detection in

IoT Systems. International Journal of Communication Networks and Information Security (IJCNIS), 13(3), 582–595.

[11] Naveen Sai Bommina , Nandipati Sai Akash, Uppu Lokesh , Dr. Hussain Syed , Dr. Syed Umar, "Multi-Objective Genetic Algorithms for Secure Routing and Data Privacy in IoT Networks", International Journal of Communication Networks and Information Security (IJCNIS), (2020), 12(3), 632–643.

[12] S. Shamshirband, M. Fathi, A. T. Chronopoulos, A. Montieri, F. Palumbo, and A. Pescapè, ―Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review, taxonomy, and open research issues,‖ Journal of Information Security and Applications, vol. 55, p. 102582, Dec. 2020, doi: 10.1016/J.JISA.2020.102582.

[13] A. Bahaa, A. Abdelaziz, A. Sayed, L. Elfangary, and H. Fahmy, ―Monitoring Real Time Security Attacks for IoT Systems Using DevSecOps: A Systematic Literature Review,‖ Information 2021, Vol. 12, Page 154, vol. 12, no. 4, p. 154, Apr. 2021, doi: 10.3390/INFO12040154.

[14] P. Chouhan and R. Singh, ―Security Attacks on Cloud Computing With Possible Solution,‖ International Journal of Advanced Research in Computer Science and Software Engineering, vol. 6, no. 1, pp. 92–96, 2016, Accessed: Feb. 08, 2023. [Online]. Available: www.ijarcsse.com.

[15] S. Abidin, ―Wireless Sensor Network and Security Mechanism by Encryption‖.

[16] A. N. Jaber and S. U. Rehman, ―FCM--SVM based intrusion detection system for cloud computing environment,‖ Cluster Computing, vol. 23, no. 4, pp. 3221–3231, 2020.

[17] M. Islabudeen and M. K. Kavitha Devi, ―A Smart Approach for Intrusion Detection and Prevention System in Mobile Ad Hoc Networks Against Security Attacks,‖ Wireless Personal Communications, vol. 112, no. 1, pp. 193–224, May 2020, doi: 10.1007/S11277-019-07022-5/METRICS.

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

[19] B. Eren, Ü. Fen, B. Dergisi, and F. Türk, ―Analysis of Intrusion Detection Systems in UNSW-NB15 and NSL-KDD Datasets with Machine Learning Algorithms,‖ Bitlis Eren Üniversitesi Fen Bilimleri Dergisi, vol. 12, no. 2, pp. 465–477, Jun. 2023, doi:10.17798/BITLISFEN.1240469.

[20] S. Maya, K. Ueno, and T. Nishikawa, ―dLSTM: a new approach for anomaly detection using deep learning with delayed prediction,‖ International Journal of Data Science and Analytics, vol. 8, pp. 137–164, 2019.

[21] A. Abbas, M. A. Khan, S. Latif, M. Ajaz, A. A. Shah, and J. Ahmad, ―A new ensemblebased intrusion detection system for internet of things,‖ Arabian Journal for Science and Engineering, pp. 1–15, 2021.

[22] A. Kurani, P. Doshi, A. Vakharia, and M. Shah, ―A Comprehensive Comparative Study of Artificial Neural Network (ANN) and Support Vector Machines (SVM) on Stock Forecasting,‖ Annals of Data Science, vol. 10, no. 1, pp. 183–208, Feb. 2023, doi:10.1007/S40745-021-00344-X/METRICS.