ENHANCED CLOUD COMPUTING INTRUSION DETECTION SYSTEM EMPLOYING DIFFERENT CLASSIFIERS

Prabhuta Dubey
Assistant Professor, EE Department, Sunrise institute of Engineering Technology and Management, Unnao, India. Email: dprabhuta7@gmail.com
Soumya Kanti Mandal
_Exicutive MTech AI and Data Science, Indian institute of information technology kalyani. Email: 1038mto23_soumya@iiitkalyani.ac.in

Abstract—Cloud computing has revolutionized the technical landscape due to its affordability and scalability. However, it has also resulted in unique security challenges. System Aided Design (SAD) has emerged as a crucial instrument for addressing security issues specific to cloud environments by enhancing the classification of these issues. Cloud computing offers cost advantages and flexibility, but because so much sensitive data is involved, privacy and data security are problems. Intrusion detection systems (IDSs), although crucial to cloud security, face challenges due to the dynamic nature of the cloud. The objective of this research project is to develop a cloud-based intrusion detection system (IDS) that uses neuro-swarm intelligence techniques to efficiently analyze and classify network traffic while adapting to the always changing cloud environment. This approach seems like a good way to safeguard data and ensure secure cloud operations. An extensive evaluation of an intrusion detection system (IDS) that employs G-ABC and DNN approaches has been conducted as part of this research effort. Additionally, this study assesses the IDS's ability to identify U2R, R2L, and Probes attacks in addition to the well-known DoS attacks using the NSL KDD and UNSW NB15 datasets. The accuracy, precision, recall, and F-measure metrics of the investigation show how the IDS may enhance intrusion detection for various attack types.

The Deep Neural Network (DNN) consistently performs the best; it retains the highest accuracy, excels in precision, balances precision and recall, and achieves high recall while minimizing false positives. This demonstrates how well DNN identifies and mitigates cyberthreats while reducing false alarms, strengthening its position in cyber security.

INDEX - **Intrusion Detection Systems, Cloud Computing, Deep Learning, NSL, Metrics, etc.**

I. INTRODUCTION

Cloud computing (CC) has always been of interest to researchers. In its early years, starting in 2008, cloud computing was defined as an execution unit with fast execution capacity. Later, as cloud and application architecture evolved, the cloud also started to provide services linked to infrastructure. The three computational levels that comprise the cloud are Infrastructure as Service (IaaS), Platform as Service (PaaS), and Software as Service (SaaS) [1]. IaaS encompasses all of the hardware-oriented procedures that make up the physical components of the cloud. IaaS, for example, will have super end processors, task scheduling units, and a negotiator who collaborates with the client to establish Service Level Agreements (SLAs). PaaS services must be coupled to provide SaaS since any application that want to function on any type of infrastructure requires an operating system platform. Cloud networks' increasing user counts have raised several security issues, including maintaining service level agreements (SLAs), managing energy efficiency in service delivery, and preventing overload on cloud execution components like physical machines (PMs). The security architecture of any computing platform may be easily separated into two components. The first is the provisioning of user authentication and the popular Role Based Access Control (RBAC) access control architecture [2]. The RBAC mechanism must be implemented by the cloud in order to guarantee that the appropriate information reaches the appropriate person at the appropriate level. The proposed effort concentrates on the second aspect of security, even though scholars from all over the world have made significant contributions to the first aspect, which is fascinating to study. The second component of network level security is the anonymous number of queries that are sent to the cloud server every second.

As a result of data science advancements, the fruit of knowledge has also produced poisons to cloud compute models, which this study publication calls security threats. Because there are so many users, it is challenging to manually identify and flag security issues, even when there are many different kinds. If a cloud doesn't identify the problem early on, there could be serious financial consequences. The hacker may briefly misuse it against a particular group of people, or they may obtain access to private accounts and reveal a lot of information. The only method to identify security threats or assaults early in such a scenario is through System Aided Design (SAD). Any SAD architecture consists of two parts: training and classification. The classification score indicates how accurate the training was. Part of the training process involves choosing data with features and feature vectors that are suitable for their category. This study document shows a new selection procedure that improves the overall classification rate for a variety of attacks [3].

Cloud-Based Computing

Cloud computing is a platform that offers virtualized resources as a pay-per-use service, much like power is distributed in an electrical grid [4]. Websites and web-based applications were installed on a single system prior to this configuration. The resources were grouped together as a virtual computer as this technology developed. One of the benefits of cloud computing for businesses is the ability to connect and interact globally without having to construct additional infrastructure, such as servers, datacenters, and other facilities. Because of its scalability, the environment can support a large number of people. The primary benefits of using this computing paradigm are lower costs, less reliance on staff, strong scalability, and other benefits [5]. Cloud computing encompasses social networking and other interactive technologies, even though it is commonly associated with the usage of internet software applications, data management, and computer capacity. Without purchasing additional gear, hiring more employees, or purchasing software licenses, cloud computing enables the dynamic reduction of congestion or enhancement of capabilities. It increases information technology's (IT) potential. Over the past few years, cloud computing has evolved from a potential business idea to one of the IT sectors with the greatest growth rates. However, as more and more commercial and personal data is kept on cloud servers, concerns about environmental security are beginning to surface.

CC has revolutionized information processing by providing a scalable, economical, and effective technical platform. From an administrative standpoint, cloud computing offers more processing and storage capacity at a lower cost. By 2024, the global cloud computing industry is anticipated to grow at a compound annual growth rate (CAGR), per an industry Research Media report [6]. However, it is more challenging to prevent and look into cloud-based crimes and assaults against clouds and their users due to the elements that make cloud computing so strong.

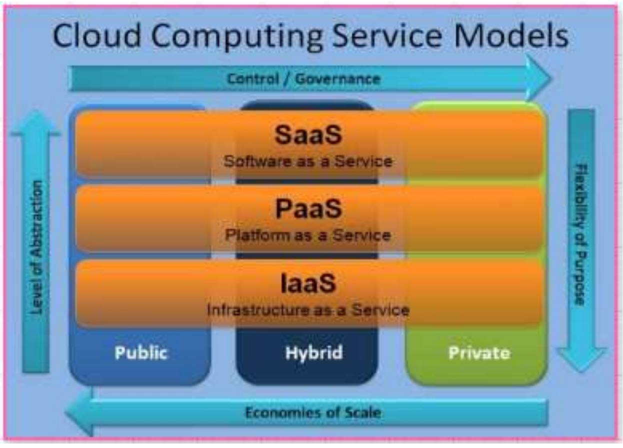

Figure 1: Cloud Computing Service Models

Cloud computing is an on-demand, pay-per-use computer architecture that offers computational resources as services via the Internet. This technology allows users to access preconfigured, low-cost hardware and software resources that are hosted and controlled remotely by a Cloud Service Provider (CSP). Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Software as a Service (SaaS) are the three service models that cloud computing offers, as shown in Figure 1 [7].

Intrusion Detection System (IDS)

Intrusion detection is the term used to describe the hardware and software systems that monitor network activity and spot security flaws in the form of malicious activity. Shortly after Dorothy Denning's work on the first intrusion detection system (IDS) model was published at SRI International, a number of IDS works were proposed to address the problems facing the research sector [8]. Figure 2 shows the generic architecture of the IDS system, which included the following components:

- The sensors that are responsible for gathering and collecting the data from the system that is being monitored.
- The detector, which is sometimes referred to as an intrusion detection engine, evaluates the data collected from the sensor in order to identify any harmful activity that may have occurred.
- Knowledgebase is a database that serves as a repository for the pre-processed version of the information that was gathered through the use of sensors. In addition, it is annotated for the attack signature, profiles, and other information that can assist security professionals.
- Information regarding the present state of the intrusion detection system (IDS) can be shared through the configuration device.
- The Response Component is the final component of the system, and it is responsible for initiating action whenever the system detects an incursion. Individualization of the generated response is possible, and it may or may not entail the participation of human beings.

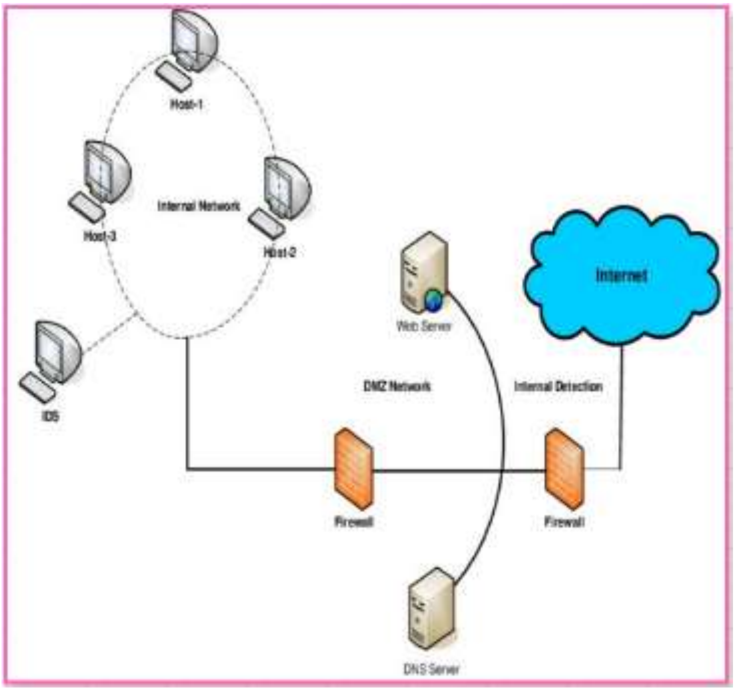

Figure 2: Intrusion Detection System

The following is a general classification of these intrusion detection technologies, also known as intrusion detection systems (IDS), which are designed to identify potential security risks in real-time scenarios [9].

Network-based intrusion detection systems (NIDS)

Network intrusion detection systems, also known as NIDS, are installed at a specific position inside the network infrastructure in order to do traffic analysis on each and every device that is connected to the network. Observations are made of the passing traffic over the entire subnet, and this traffic is compared to a list of attacks that are already known. It is possible for the administrator to receive the notification as soon as an assault is identified or when suspicious activity is observed. Examples of Network Intrusion Detection Systems (NIDS) include the installation of an NIDS on the subnet where firewalls are located in order to identify attempts to breach the firewall.

Host-based intrusion detection systems (HIDS)

It is possible for host intrusion detection systems, sometimes known as HIDS, to function on distinct hosts or network devices. Only the incoming and outgoing packets of the device are monitored by a high-level intrusion detection system (HIDS), which alerts the administrator to any suspicious or malicious activity that may occur. A snapshot of the system files that are currently present is taken, and then a comparison is made between those files and the most recent snapshot. The administrator receives a notification so that they can investigate any modifications or deletions that have been made to the files that make up the analytical system. The utilization of HIDS is demonstrated on machines that are considered mission-critical, and it is not anticipated that their configuration will be altered.

System for Detecting Intrusions That Is Hybrid: The term "hybrid intrusion detection system" refers to a system that is created by combining two or more traditional methods of intrusion detection. The information about the network is combined with data from the host agent or the system by the hybrid intrusion detection system. This allows for the creation of a comprehensive picture of the network system. The hybrid intrusion detection system is more effective than other intrusion detection systems when these systems are compared to one another. Prelude is an example of a hybrid intrusion detection system.

Intrusion Detection System in Network Security

It is the following functions of IDS that have contributed to its widespread popularity among its many customers:

- It monitors the tasks that are being performed by routers, firewalls, key management servers, and files throughout the network.
- It gives users constant support throughout the entire process.
- Organises the numerous audit trails and other logs that are available.
- It will sound an alarm whenever there is a break in security that is discovered.
- Once they have identified the potentially malicious behavior, they promptly prohibit access to the server.

Method of Detection Utilizing IDS

Signature-Based Method: Signature-based intrusion detection systems are able to identify attacks by paying attention to specific patterns, such as the number of bytes, the number of ones, or the number of zeros that are present in the network traffic. This allows the systems to identify attacks. Additionally, it is able to recognize harmful software by examining the sequence of instructions that is already known to be exploited by malicious software [10]. This allows it to identify dangerous software. There are patterns that are recognized by the intrusion detection system (IDS), and these patterns are known as signatures. Intrusion detection systems that are based on signatures are able to detect attacks with relative ease if the pattern (signature) of the attack is already present in the system. However, it is quite tough to identify new malware attacks because the pattern (signature) of these attacks is unknown.

Method Based on Anomalies: Because of the quick rate at which new malware is being created, anomaly-based intrusion detection systems were developed in order to identify attacks that arise from malware that is not previously known. The generation of a trustworthy activity model is accomplished by the application of machine learning in the process of putting into action an anomaly-based intrusion detection system (IDS). When any new information is received, it is compared to this model, and if it is not included in the model, it is considered to be suspicious [11]. A superior generalized property is possessed by the technique that is based on machine learning in comparison to the intrusion detection system (IDS) that is based on signatures. This is as a result of the fact that these models can be trained in accordance with the parameters of the hardware and the applications.

II. LITERATURE SURVEY

Utilizing cloud computing, which includes monitoring tools, storage tools, analytics tools, visualization platforms, and client delivery, makes it possible to perform utility computing. Organizations and individuals will be able to have on-demand access to a wide selection of helpful applications from any location thanks to the subscription-based pricing model that cloud computing utilizes. When it comes to cloud computing, which is now widely utilized for the transfer of sensitive information all over the world, information sharing is the most important aspect. Due to the fact that this information is accessible to all users, data that is stored in the cloud is susceptible to security breaches [12]. There are a great number of hackers who are attempting to exploit the cloud's facilities and overcome its security. There is a severe problem with the security breach, which has the potential to interrupt cloud services. A wide range of methods are utilized by hackers in order to prevent users from gaining access to data that is kept in the cloud.

Raghav Bang et al. [13] discussed an intrusion detection system (IDS) that was proposed in a novel manner that makes extensive use of the cross-layer interaction.In an ideal scenario, the approach would provide IDS to each layer of the OSI model. It is offered for single cross layers IDS to numerous layers of the OSI model. At various stages of the stack protocol, wireless sensor networks (WSNs) are vulnerable to a variety of assaults. When it comes to WSNs, numerous IDS were designed. The OSI model utilizes a single layer for the operation of these systems. These layers' ability to work together and interact with one another was taken into consideration. These systems are inefficient, and the WSN becomes depleted as a result of their presence. The problem is tackled with intrusion detection systems in a different way, and the cross-layer concept is used extensively, which results in the birth of a new form of intrusion detection system.

In their discussion of the business sector network, Yadav, T. et al. [14] pointed out that intrusion detection is a highly essential technology in the study field. This weapon is highly effective and provides a high level of information security. IDS is utilized for the purpose of monitoring a network in order to report any intrusions that occur to the administrator so that they can take the necessary actions. Computers that are able to communicate with several buildings that are located thousands of miles apart are the building blocks of networked distributed systems like these.The system that possesses the network is the one that decides the conduit via which scattered systems and computers can communicate with one another. This method was developed in order to identify assaults on network systems, such as SYN flooding and IP spoofing, among other types of attacks.Using a signature-based intrusion detection system (IDS) methodology, it then proceeds to establish the attacks. Using signature-based intrusion detection systems (IDS) to monitor the packets on the network and then matching those packets to the characteristics of known malicious assaults is examined in this article. This system will often present the list of attacks to the administrator for any confusing actions that may be taken. During the course of an assault, this system functions as a warning device, and it is directed toward the entire network.

In addition to M. Oswal, [15] Signature-based categories, anomaly-based signatures, and hybrid-based categories were the three categories that were generally used to classify intrusion detection systems (IDS). These intrusion detection systems each have their own set of benefits and drawbacks. If the anomaly-based intrusion detection system (IDS) is calibrated correctly, it is able to identify novel attacks even if it is unaware of the payload contents. In most cases, the pace of data packets is what determines how an IDS operates. The most significant drawback is that it generates a significant number of false positives, in contrast to signature-based intrusion detection systems, which do not generate false positives. Furthermore, these systems are unable to identify new attacks until their database is updated. A hybrid intrusion detection system (IDS) combines the characteristics of signature-based IDS with anomaly-based IDS. A description of the implementation of the kind of intrusion detection system (IDS) is provided in this work. Additionally, performance may be evaluated based on the consumption of random access memory (RAM), demonstrating that the detection method uses less RAM than SNORT.

In a study that was carried out by Celesty Gedam et al. (2020), a deep learning-based Feedforward Neural Network (FFNN) classifier was utilized to evaluate the classification performance on the UNSW-NB15 and NSL-KDD datasets. It was decided to take into account the findings of this evaluation. It was determined, on the basis of the findings of the research, which adopting a large feature set could result in features that are redundant and superfluous, which would take a significant amount of computational resources. This was discovered. On the other hand, the proposed method, which made use of a very tiny feature vector, resulted in a significant improvement in classification accuracy. This was the case since the feature vector was quite small. An incredible 91.29% accuracy was attained within the setting of the UNSW-NB15 dataset. This was a remarkable achievement. The classifier demonstrated an amazing accuracy of 89.03% when it was applied to the NSL-KDD dataset, which is comparable to the example that was presented earlier. These results, which emphasize the usefulness of the technique, revealed that the method was effective in locating network traffic irregularities in these datasets. [16] More specifically, the results demonstrated that the method was effective.

In order to recognize malicious software that is present in cloud networks, Suruchi Dedgaonkar et al. (2020) have applied an algorithm for machine learning through their research. Particle Swarm Optimization (PSO), which is a bioinspired method, has been applied to improve the characteristics that are utilized to detect malware assaults. These features improve the detection of malware attacks. There were a total of 3500 bebigs, and the system utilized 5000 Drebin malware at the same time. According to the findings of the experiment [17], the AdaBoost classifier had a True Positive Rate (TPR) of 95.6% when it comes to identifying malicious software.

III. METHODOLOGY

As a result of the fact that the proposed algorithm is going to be used to build a SAD-based architecture, it is essential for them to have both a training mechanism and a classification mechanism. As a consequence of this, the objective that has been decided upon is to carry out an investigation into the data security based on the classifiers. There are four techniques that have been selected for training and classification in order to achieve this objective. These algorithms include Deep Neural Networks (DNN), Back Propagation Neural Networks (BPNN), Support Vector Machines (SVM), and Naïve Bayes (NB). The selection of these strategies was based on the research that has been done. In addition, the study that was proposed attempted to conduct out a survey on the classification accuracy of the classifiers without making any changes to the dataset. Each of these four approaches has a training architecture that is distinct from the others. This target will address both of the difficulties that have been identified. When the classification accuracy of the dataset is less than fifty percent, this suggests that the data requires a considerable amount of pre-processing in terms of the identification of distinguishing characteristics. To begin, this is an indication that the data needs to be processed. Moreover, it would be able to handle the problem of selecting the classifiers that are the most appropriate for these datasets, which is the second difficulty. The use of the work flow diagram that is presented in Figure 3 is one method that can be utilized to illustrate the general flow of work.

Support Vector Machine (SVM)

There are many different domains in which the Support Vector Machine (SVM), a well-known supervised learning technology, has proven to be an extremely effective solution for classification and regression issues. Fetal well-being monitoring is one of the numerous disciplines in which this technology has been utilized. Finding kernels that are more efficient in order to further enhance accuracy is the primary emphasis of the current research endeavors, whereas a significant percentage of the previous research efforts were concentrated on enhancing SVM learning algorithms [18]. It is possible that classic kernels like as linear, polynomial, and Gaussian kernels do not sufficiently capture the nuances of specific datasets, despite the fact that they are beneficial. As a consequence of this, the research community is currently conducting extensive research on new kernel functions that have the potential to be utilized in signal processing and multimedia applications. In contrast to the complex methods that are utilized in deep learning, kernels offer a strategic approach that is more effective and play a significant role in determining how well a support vector machine (SVM) functions. In their most basic form, these kernels are mathematical processes that are designed to convert non-linearly separable input data into linearly separable data in an environment with a higher dimension. A kernel function, in its most basic form, is able to compute the inner product between two data points in a suitable feature space in order to generate a measure of similarity without incurring any additional processing cost. This is true even when dealing with extremely high-dimensional data.

A "kernel," which is also commonly referred to as the "kernel trick," is a strategy that is utilized within the field of machine learning. This technique utilizes a linear classifier in order to solve issues that are essentially non-linear in nature. Through the use of this technology, data that cannot be separated linearly are transformed into a format that allows for linear separation to be performed. The kernel function, which is applied to each data instance, is the most important part of the process. It is responsible for allowing the transition of the initial non-linear observations into a higher-dimensional space, which allows for the effective differentiation and separation of these observations.

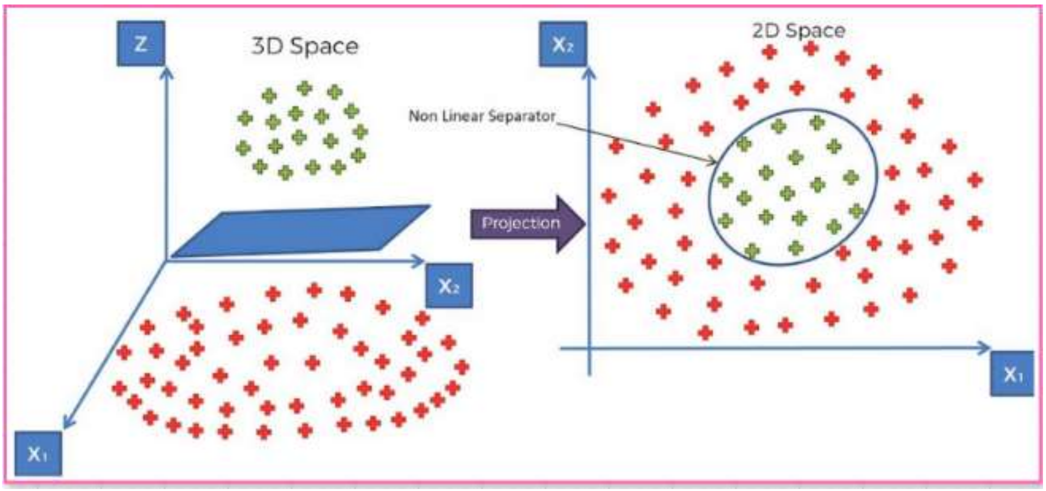

Figure 3: Nonlinear Data

As can be seen in Figure 5, the endeavor of attempting to construct a linear border within the input space for the purpose of distinguishing lemons from apples is a hurdle that cannot be overcome. The data, on the other hand, can be projected into a higher-dimensional realm, as shown in the feature space of the image that was explained before. This makes it possible to locate a hyperplane that effectively classifies the data. The kernel technique makes a substantial contribution to the process of locating such a hyperplane within this space with higher dimensions, while at the same time keeping relatively low processing costs. This is how the kernel trick contributes to the process. The conventional kernels, on the other hand, have limitations in their power to discern between particular sorts of datasets, which results in a loss in performance in circumstances like these. Both of these kernel functions have significant drawbacks that need to be taken into consideration. In the first place, they simply simulate the inner product between individual feature vectors, rather than taking into consideration an ensemble of vectors. This is a significant limitation. Second, they are not very specialized and do not make use of the unique statistical qualities of the specific signals that are being studied. This is a significant limitation.

Artificial Neural Networks (ANN)

Within the framework of a neural network, simple processing components that are assigned weights are connected to one another. Both architectural and information processing logics are going to be utilized in order to achieve the goal of accurately representing the nervous system in biology. In Figure 4, the architecture of the neural network is depicted. This network needs to go through training before it can proceed with the application of an efficient learning technique for the prediction of connected weights. The signals are categorized when the weight test training has been completed [19]. In the realm of neural networks, the multilayer perceptron network is a type of network that is primarily utilized for classification procedures.

The number of hidden layers, as well as the number of inputs, outputs, and hidden neurons, are all components that are included in the definition of an artificial neural network (ANN) architecture [18]. A feed-forward network with a single hidden layer and a finite number of neurons can estimate continuous functions on compact subsets of Rn, where n is the number of inputs, according to the universal approximation theorem [20]. This theorem asserts that the network can approximate continuous functions. On the other hand, this does not imply that an artificial neural network (ANN) with a single hidden layer should be considered the best in terms of adaptability, learning time, and ease of implementation. Given the sets of input and output data, there is no general rule that can be used to identify the optimal architecture for an artificial neural network (in terms of the number of neurons and hidden layers). We present here an approach that is based on trial and error and is intended to calibrate the architecture of the

ANN in accordance with the complexity of each individual scenario. The process is broken down into two stages: first, a crude calibration is performed in order to ascertain the number of hidden layers; second, training is performed with a rising number of hidden neurons (beginning with a few of them) until the desired level of performance is achieved.

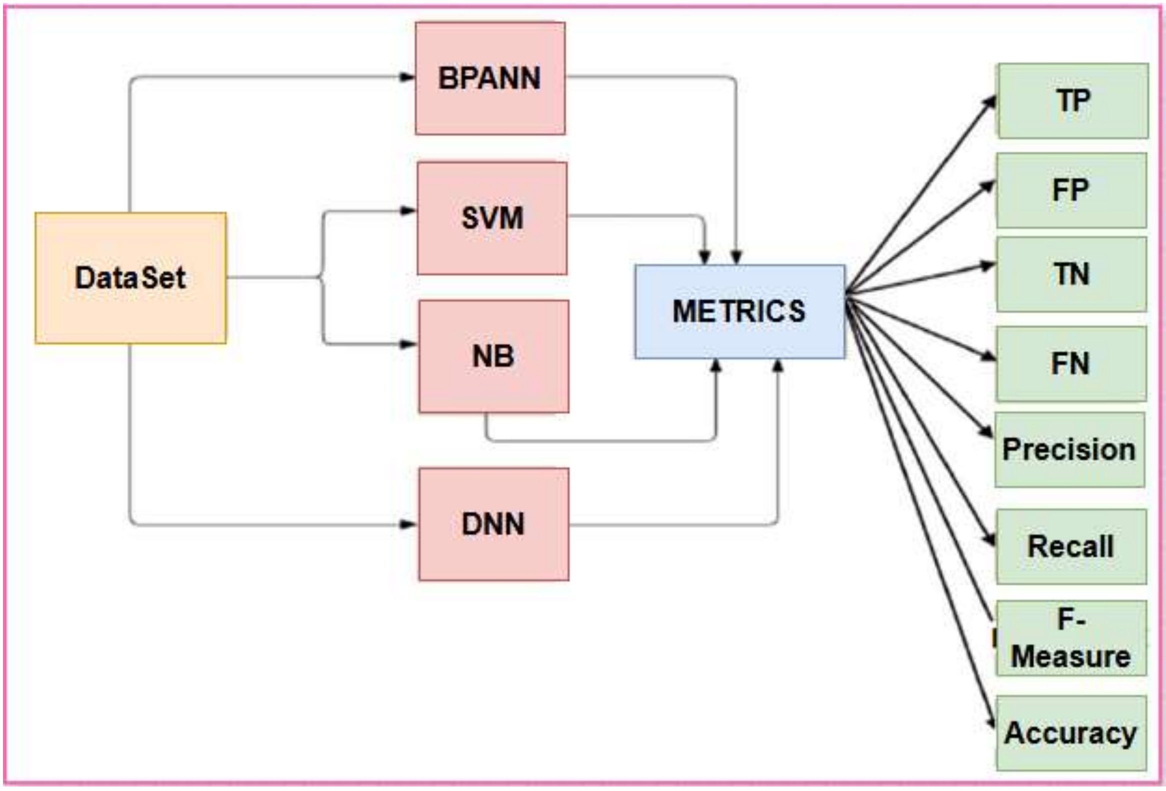

Figure 4: The general block diagram

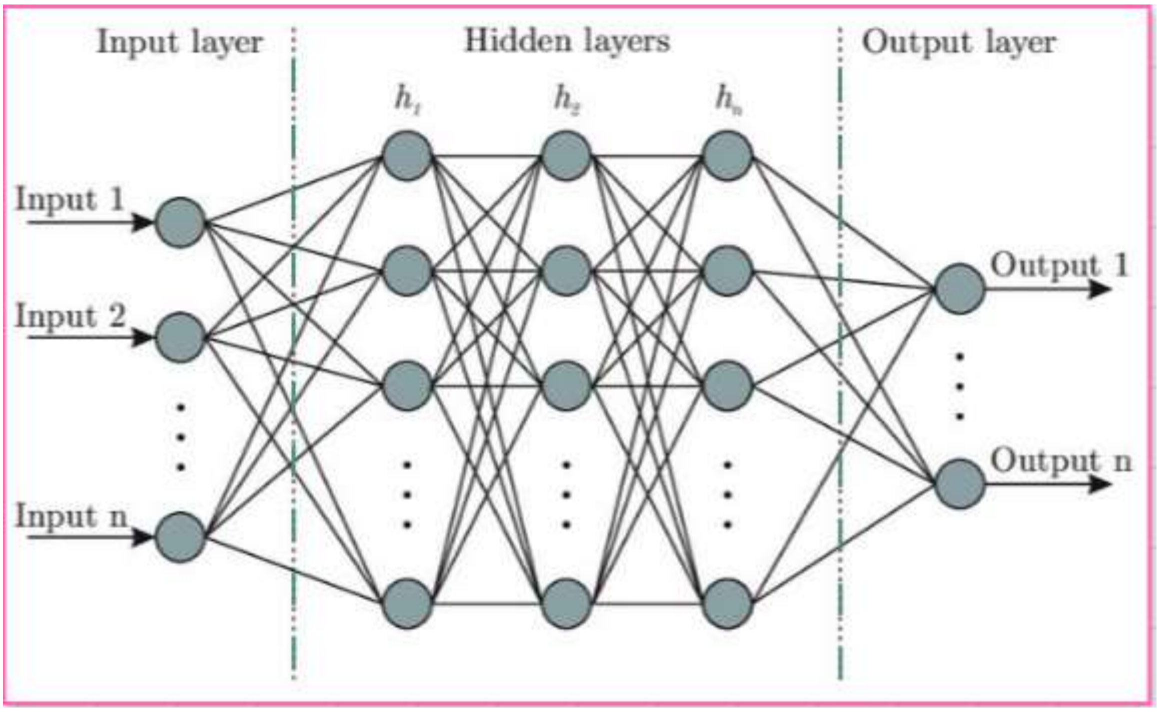

Figure 5: Neural Network Architecture

Deep Neural Networks (DNNs)

Deep neural networks (DNNs), which are artificial neural networks that consist of multiple layers of neurons, have the ability to learn and mimic complex connections between the data that is presented to them and the outputs that are desired. In this article, we will investigate deep neural networks (DNNs) and their applicability to a variety of tasks, such as speech recognition, picture categorization, and natural language processing, which are all depicted in Figure 6 [21].

It is helpful to begin with a single artificial neuron, which is a straightforward mathematical model that can be utilized to carry out binary classification tasks, in order to gain an understanding of deep neural networks (DNNs). A single artificial neuron receives a number of inputs and then employs a weighted sum to generate an output. This output is then processed through an activation function in order to get the final prediction.

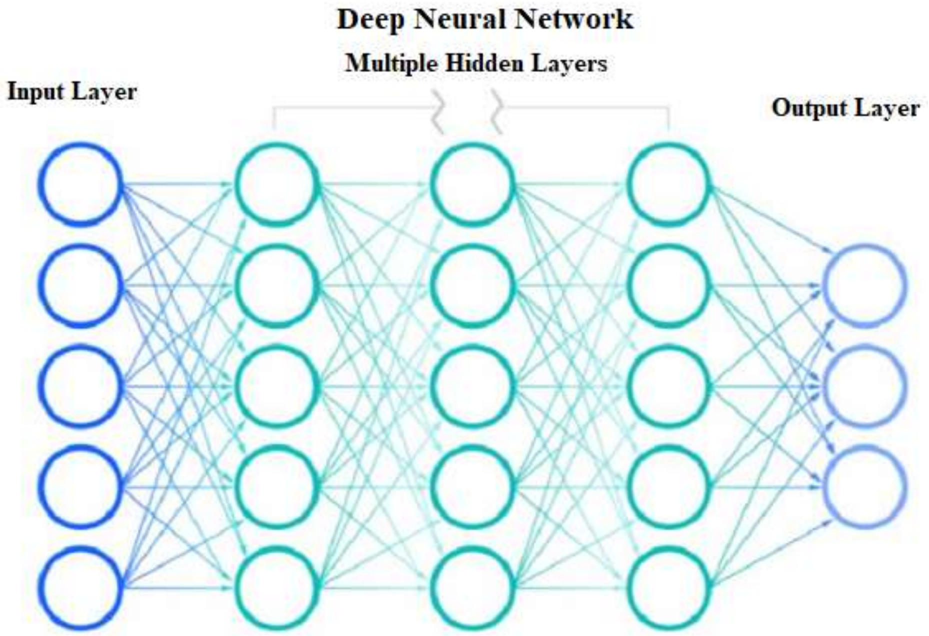

Figure 6: Deep Neural Network along with Multiple Hidden Layers

The results of the layer that comes before it are processed in order to generate the output of each layer in a deep neural network (DNN). This output is then transmitted to the layer that comes after it. The initial layer is the input layer, for which it is responsible for receiving raw data. Finally, the final layer is the result of this layer, which is responsible for generating the final forecast. All of the layers that are located in between are referred to as hidden layers, and their primary function is to enable higher-level computations and the extraction of features from the data [22].

IV. RESULTS AND ANALYSIS

The average precision values for four different classifiers, namely SVM, FFBPNN, and DNN, have been observed to be consistent over a wide range of cyber-attack techniques. Precision is an essential indicator in the field of cybersecurity since it evaluates the precision of positive predictions and ensures the dependability of alerts or alarms that are generated by a model. Particularly noteworthy is the fact that the suggested DNN classifier excels with an average precision of 0.9501, indicating the highest precision across a wide range of attack types. This demonstrates that DNN has an extraordinary capacity to efficiently reduce the number of false positive mistakes, which makes it a reliable option for intrusion detection.

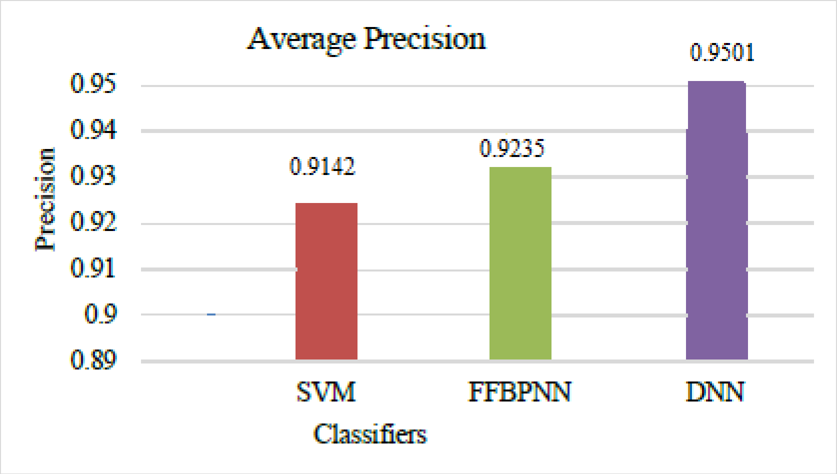

Figure 7: Precision Analysis

As a crucial indicator, accuracy provides a thorough picture of how well a classifier can accurately categorize attacks and non-attacks across all classes. Accuracy is a measure of how well a classifier can classify classes. With regard to the various classifiers and assaults, the average accuracy analysis is presented in Figure 7. With an impressively high average accuracy of 95.713%, the DNN classifier that was presented stands out as particularly impressive. When it comes to successfully recognizing cyber threats and non-threats across a wide range of attack types, DNN is the clear winner thanks to its outstanding accuracy score, which demonstrates its overall dominance.

V. CONCLUSION

In this study, a comparative analysis is presented to demonstrate the efficacy of several classifiers in protecting against a variety of assaults. The evaluation is carried out by employing a variety of attacks derived from two Average Accuracy datasets, specifically the NSL-KDD datasets employed. SVM, FFBPNN, and DNN are the classifiers that were utilized in the analysis. These classifiers were tested for their detection precision, recall, f-measure, and accuracy for various cloud attacks that impact network security. Based on the findings of the comprehensive investigation, it has been determined that the DNN architecture exhibits a considerably high level of intrusion detection strength. As a result, it has been incorporated into the proposed intrusion detection system as a machine learning classifier.

REFERENCES

[1] T. Guarda, M. F. Augusto, I. Costa, P. Oliveira, D. Villao, and M. Leon, ―The Impact of Cloud Computing and Virtualization on Business,‖ Communications in Computer and Information Science, vol. 1485, pp. 399–412, 2021, doi: 10.1007/978-3-030-90241-4_31/COVER.

[2] Habeeb, M. S., & Babu, T. R. (2022). Network intrusion detection system: a survey on artificial intelligence-based techniques. Expert Systems, 39(9), e13066.

[3] Prema Latha , V., Dinesh Kumar, A., & Parveen, N. (2025). Optimizing interactions: Strategies for prompt engineering in large language models. Edu - Tech Enterprise, 3, 24. https://doi.org/10.71459/edutech202524

[4] Habeeb, M. S., & Babu, T. R. (2024). Coarse and fine feature selection for network intrusion detection systems (IDS) in IoT networks. Transactions on Emerging Telecommunications Technologies, 35(4), e4961.

[5] K. Kartheeban, K. Kalyani, S. K. Bommavaram, D. Rohatgi, M. N. Kathiravan, and S. Saravanan, “Intelligent Deep Residual Network based Brain Tumor Detection and Classification,” in 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS), Dec. 2022, pp. 785–790. doi:10.1109/ICACRS55517.2022.10029146.

[6] Habeeb, M. S. (2024). Predictive analytics and cybersecurity. Intelligent Techniques for Predictive Data Analytics, 151-169.

[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] 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.

[9] Usman, M., Zubair, M., Hussein, H. S., Wajid, M., Farrag, M., Ali, S. J., ... & Habeeb, M. S. (2021). Empirical mode decomposition for analysis and filtering of speech signals. IEEE Canadian Journal of Electrical and Computer Engineering, 44(3), 343-349.

[10] M. Mukhedkar, D. Rohatgi, V.A. Vuyyuru, K.V.S.S. Ramakrishna, Y.A. Baker El-Ebiary, V.A. Asir Daniel, "Feline wolf net: A hybrid lion-grey wolf optimization deep learning model for ovarian cancer detection", Int. J. Adv. Comput. Sci. Appl., 14 (9) (2023)

[11] Premalatha, V., Parveen, N. Adaptive fish school search optimized resnet for multi-view 3D objects reconstruction. Multimed Tools Appl 83, 77639–77666 (2024). https://doi.org/10.1007/s11042-024-18530-3.

[12] Chandankhede, C., Sachdeo, R. Offline MODI script character recognition using deep learning techniques. Multimed Tools Appl 82, 21045–21056 (2023). https://doi.org/10.1007/s11042-023-14476-0.

[13] Raghav Bang, Manish Patel, Vasu Garg, Vishal Kasa, Jyoti Malhotra and Sambhaji Sarode, "Redefining smartness in township with Internet of Things & Artificial Intelligence: Dholera city" E3S Web Conf., 170 (2020) 06001, DOI: https://doi.org/10.1051/e3sconf/202017006001.

[14] Yadav, T., & Sachdeo, R. (2024). Enhanced face age progression and regression model using hyper-parameter tuning-large scale GAN by hybrid heuristic improvement. The Imaging Science Journal, 72(8), 1126–1146. https://doi.org/10.1080/13682199.2023.2254134

[15] M. Oswal, K. Mahajan, S. Pagare, V. Kasa, J. Malhotra and S. Sarode, "Feature-Based Analytical Crop Recommendation System," 2021 IEEE Pune Section International Conference (PuneCon), Pune, India, 2021, pp. 1-6, doi: 10.1109/PuneCon52575.2021.9686530.

[16] Celesty Gedam, Madhavi Sahare, Rajneeshkaur Sachdeo and Nilima Kulkarni, "Smart Transportation Based Car Pooling System", E3S Web Conf., 170 (2020) 03004. DOI: https://doi.org/10.1051/e3sconf/202017003004

[17] Suruchi Dedgaonkar, Rajneesh Kaur Sachdeva-Bedi, Kunil Kothari, Riya Loya, Suneel Godbole, "Role of IoT and ML for autistic people", International Journal of Future Generation Communication and Networking. Vol. 13, No. 3s, (2020), pp. 773–781.

[18] Vickranth V.;Bommareddy S.;Premalatha V., "Application of lean techniques, enterprise resource planning and artificial intelligence in construction project management", International Journal of Recent Technology and Engineering, Volume 7, Year 2019, Pages 147-153

[19] PremaLatha V.;Sreedevi E., "Cogitation on Agents of Things (AOT) of Internet of Things (IOT)", Journal of Advanced Research in Dynamical and Control Systems, Volume 9, Year 2017, Pages 654-663.

[20] Premalatha V.;Vineesha K.;Srinivasarao M., "Recon approach for social dynamics based on agent model", International Journal of Scientific and Technology Research, Volume 9, Year 2020, Pages 1005-1008.

[21] Premalatha V.;Anguraj D.K.;Parveen N., "Integrated neural-hybrid system for efficient tumor detection and object reconstruction", Data and Metadata, Volume 4, Year 2025, DOI:10.56294/dm2025850.