SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V12I3P108

Volume 12 Issue 3, 88-100, March 2025

Original Article

Enhanced Deep Learning-Based Security Model for Data in Cloud

Gantela Prabhakar[1], Bobba Basaveswara Rao[2]

[1,2]*Department of Computer Science Engineering, Acharya Nagarjuna University, Guntur, Andhra Pradesh, India.*

[1]*Corresponding Author : gantelaprabhakar@gmail.com*

Received: 06 January 2025 Revised: 06 February 2025 Accepted: 08 March 2025 Published: 29 March 2025

Abstract *- Nowadays, numerous cloud services are available for companies of all sizes and types. It can be used for virtual workstations, analysis, backup, and even software development. However, this ease of use is accompanied by security risks. The technology's limitations make information security a major concern for cloud computing. A comprehensive set of technical solutions, policies, and procedures for safeguarding cloud-based systems or applications, as well as user access and data rights, are known as cloud security. Data availability, integrity, and confidentiality are fundamental concepts in information security. For companies of all sizes and types, a variety of cloud services are now available. By sorting the jobs in each data set and choosing the ones with the highest scores, choose only the most pertinent ones. The proposed Convolutional Neural Network (CNN)-BI-LSTM's accuracy was tested, trained on, and validated using the CICDDoS2019 dataset, which had a 94.52% accuracy rate. A Kalman neural network with back-propagation has been utilized to detect Distribution Denial of Service (DDoS) in IoT networks compatible with 5G. The recall rating for this model was the highest (0.9749). The highest accuracy score, 0.954, was achieved by IDS based on convolutional neural networks. Finally, combine a model that more precisely and effectively detects and categorizes DDoS assaults in a multi-control SDN with an entropy-based deep learning approach. According to the experiment's findings, Recurrent Neural Networks (RNN) had an accuracy of 98.6%, Multi-Layer Perceptron (MLP) had 98.3%, Gated Recurrent Unit (GRU) had 96.4%, and LSTM had 99.42%. Among other suggested models, the Long Short-Term Memory (LSTM) demonstrated great accuracy. To address these problems and offer a defense against sophisticated threats, an innovative deep-learning methodology was developed. Many of these issues can be resolved using new ideas and methods in cyber security, such as speech recognition, behavioral anomaly detection, malware, botnet detection, and DDoS detection. We introduce a secure and fair distributed deep learning architecture that solves the problems mentioned above and improves data security in the cloud.*

Keywords *- Convolutional Neural Network, Distributed Denial of Service, Multi-Layer Perceptron, Long Short-Term Memory, Back-propagation.*

1. Introduction

Google's CEO, Eric Schmidt coined the term "cloud computing" in late 2006. Cloud computing, a key component of the fourth industrial revolution, is now widely regarded as the most cutting-edge technology in developed countries [1]. Cloud computing security also concerns elements of intricate infrastructures [2]. With the use of specialized information processing technologies, users of cloud computing can request Internet services based on the capacities of their computer systems. Because users are unaware of the internal configuration of cloud computing, they have flexibility.

A cloud infrastructure includes physical data storage and a virtual setting. Threats to cyber security can impact all facets of cloud computing [3]. Security issues are made more difficult by various cloud model components, including network, architecture, APIs, and hardware. Because of this, various combinations of cloud components expose security flaws to both the cloud provider and its users [4]. To ensure the security of cloud computing, it is essential to develop a conceptual model that includes all the necessary components [5]. In the third layer of SDN architecture, the data plane and control plane operate independently [6]. Switches and routers make up the data plane, which carries network traffic. Control planes include the NOX, POx, Beacon, and Floodlight and Open Daylighted controls. Defined Networking (SDN) setup tools make up the application layer. If the network is the target of a DDoS attack, the SDN controller won't be able to respond to regular network traffic, and the SDN will lose central control. As a result, the primary benefit of centralization within an SDN network is threatened by DDoS attacks [7]. DDoS is a helpful tool to disrupt the adversary's infrastructure and applications when a dispute arises between two people or groups. The unfairness of the attack may lead

the individual to start acting malignly and violently. A terrorist organization attempts to topple an economic system by engaging in political or geopolitical cyber warfare [9]. Figure 1 explains the various shapes that DDoS attacks.

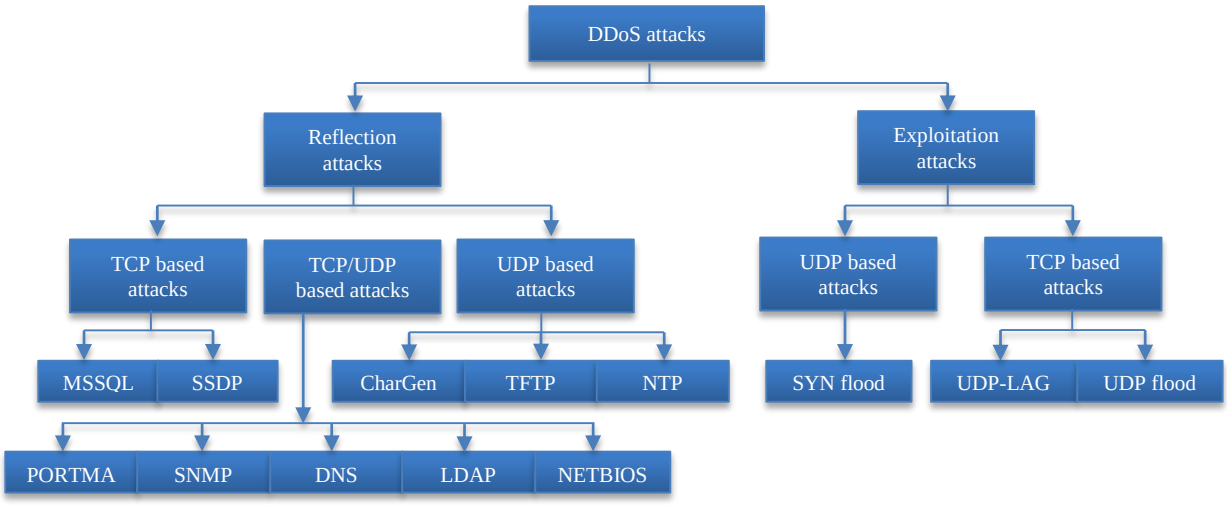

Fig. 1 Diverse approaches to DDoS attacks

In detecting and classifying DDoS attacks in multifunctional SDNs, the following problems must be solved using entropy and deep learning models: Increasing the models' precision and dependability. Deep learning still has room to improve robustness and accuracy. To enhance model performance, future research can examine various architectures, feature selection techniques, and machine learning algorithms, analyzing model performance in a practical setting. In this paper, a DDoS attack simulation was used to assess the proposed model.

Nevertheless, the model's success must be evaluated in real-life scenarios where traffic types fluctuate and the network conditions change. The model's functionality in real network environments can be evaluated in future research. False positives can be a major problem in detecting DDoS attacks, leading to network failures and wasted resources. Future studies will aid in lowering the likelihood of false positives in the model. Find out how DDoS attacks impact various network types. However, DDoS attacks in multi-control SDN setups are the main topic.

Networks such as cloud and IoT networks are susceptible to DDoS attacks. Cloud computing is a crucial technology enabling individuals to handle and share extensive data online without installing software on their devices. It enables businesses to effortlessly modify their resources, potentially lowering expenses. This technology allows companies to assess and handle applications more rapidly while needing less upkeep. Nonetheless, with increased Internet usage, security threats such as Distributed Denial-of-Service (DDoS) attacks also rise. Future research may focus on how DDoS attacks impact these diverse network types and create models that can adapt to their distinct features.

1.1. Contribution

- Considering this, invent a fresh security measure for advanced cloud computing systems incorporating multiple layers of cloud technology. The analysis of the cyber security issues of the cloud service model led to the development of the cloud security attack model.
- The laws governing cloud computing and cyber security requirements are described below. "Cybersecurity" and "cyber resilience" concerning the safety of cloud systems and the advancement of intelligent cloud computing.
- A comparison of various aspects of cloud-based identity and access management mechanisms.
- DDoS assaults can target while there are other networks, such as cloud and IoT networks. For example, multi-controller SDN is the focus of current research, which is primarily focused on DDoS attacks.

2. Literature Survey

IoT security has been the focus of in-depth research and analysis to help foresee future challenges. IoT security is a well-known research area, yet there's minimal emphasis on machine learning within this field. Research has investigated concerns such as access regulation, management of authentication processes (AES), security of applications, encryption methods, and network protection [10]. The study in [11] outlined the issues and potential fixes for IoT communication security. Another article [12] stressed the importance of IoT systems in intrusion detection. DDoS attacks employ numerous devices to interfere with online services, highlighting the importance of robust defenses. This document examines DDoS threats and defensive strategies in [13]. Cloud computing utilizes the internet to share resources, scale services, and deliver on-demand solutions without significant infrastructure expenses. The article examines its

ideas, background, virtualization, services, and research obstacles [14]. IoT legal issues and regulatory frameworks may also specify security and privacy requirements [15]. [16] discussed security and privacy issues in a distributed IoT environment. These pieces covered a wide range of topics.

Researchers emphasize that there are many issues to investigate and that a distributed IoT approach has many benefits in terms of privacy and security. [16] researched to outline the development of security threats and vulnerabilities in IoT devices, including their software. IoT context in terms of data security and privacy protection using machine learning techniques was briefly discussed by the authors of [17]. The costs of communication and computation, considerations for partial states, and backup security were also covered in the paper's discussion of three challenges related to machine learning applications in IoT environments. Research has explored the application of data mining and machine learning to identify weaknesses in cyber security [18].

They focused primarily on cyberspace anomalies and violations. With a focus on their use in IoT environments, the methodology was based on several categories of AI methods from an IoT context perspective. The review in [19] also discussed how machine learning techniques are used in IoT security challenges and current solutions. In [20], other studies on machine learning techniques for Wireless Sensor Networks (WSN) have been released. Four attack scenarios illustrate the TENNISON framework's effectiveness and capabilities. [21] et al. investigated the characteristics of the various detection methods available to stop DDoS attacks. A scalable multi-domain, multi-vendor SDN architecture was put forth by [22]. The orchestrator controller is created and implemented to enable various SDN administrative areas [23].

Establishing a multi-vendor, multi-domain pilot environment with three vendors validates this approach. The findings show that end-to-end provisioning services and network state consistency maintain consistency. [24] et al. suggested a team-based method for monitoring DDoS attacks on a distributed SDN platform with numerous controllers. Investigations of DDoS assaults that target distributed controllers in SDN networks as opposed to central controllers have also been done. Use an attack detection and mitigation monitoring system integrating Open vSwitch with the POX console.

[25] suggested leveraging benchmark data from existing models to train the use of DL CNN and Bi LSTM technology to enhance the ability to predict DDoS attacks. By sorting the jobs in the given data set and choosing the ones with the highest scores, choose only the most pertinent ones. The CNN-BI-LSTM model was developed using the CICDDoS2019 dataset and reached an accuracy of 94.52%. The analysis revealed that most studies utilized outdated datasets for their experiments. To recognize the most recent DDoS attacks, we utilized the CICDDoS2019 dataset, which contains current types of attacks. We observed that detection efficacy might be enhanced, so we integrated a well-known transformer framework to develop a new model for improved detection of DDoS attacks. Figure 2 explains the CNN-BI-LSTM model.

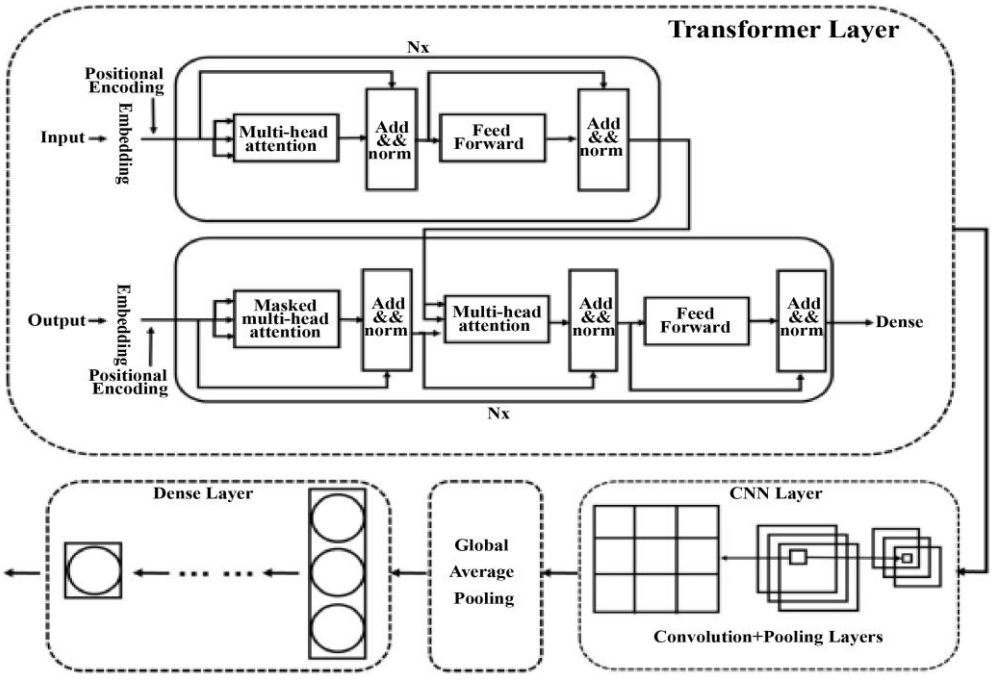

Fig. 2 CNN-BI-LSTM structure

3. Problem Statement

Create a website based on blockchain technology and find security holes in other websites to improve security. The passport registration website contains an individual's personal information. The attack on the website combined blockchain technology with a denial-of-service attack.

3.1. Problem Description

Using blockchain technology, the passport application can be submitted online. Sites on the blockchain are very secure because they are distributed and decentralized. These websites are virtually impossible to hack due to their low vulnerability. But it might be down at the bottom of the page. As these pages get more traffic, attackers are more likely to target them, and eventually, candidates won't be able to access the page. Complex safety measures will be necessary.

3.2. Cyber Security Reference Model of Intelligent Cloud Computing

Providing security for network services in the cloud system requires thorough documentation of its architecture. This is particularly important. As a result, major companies such as NIST, IBM, and Microsoft offer cloud computing benchmarks. NIST has established five benchmarks for standard information system models in cloud computing: cloud client, cloud service provider, cloud operator, cloud browser, and cloud agent. According to NIST, the reference model encompasses several layers, including instrumentation, services, physical resource and cloud service management, and information security layers. The following queries will be covered in this section.

- Resources need to be assigned and allocated to restore, update, and connect new nodes. Virtual resources need to be watched over.
- Keep an eye on cloud activity and offer performance reports.
- Standards for Service Level Agreements (SLAs); surveillance of SLA execution under established security policies

Currently, cloud computing reference models do not consider the virtualization and service layers and necessary components for fulfilling cybersecurity specifications, nor do they consider the social media (IoT) awareness layer produced by attackers.

There are no cyber resilience issues with cloud computing or cloud services. This task proposes a novel cyber security reference framework for cloud computing systems, addressing all tiers. The new model is shown in Figure 3 below.

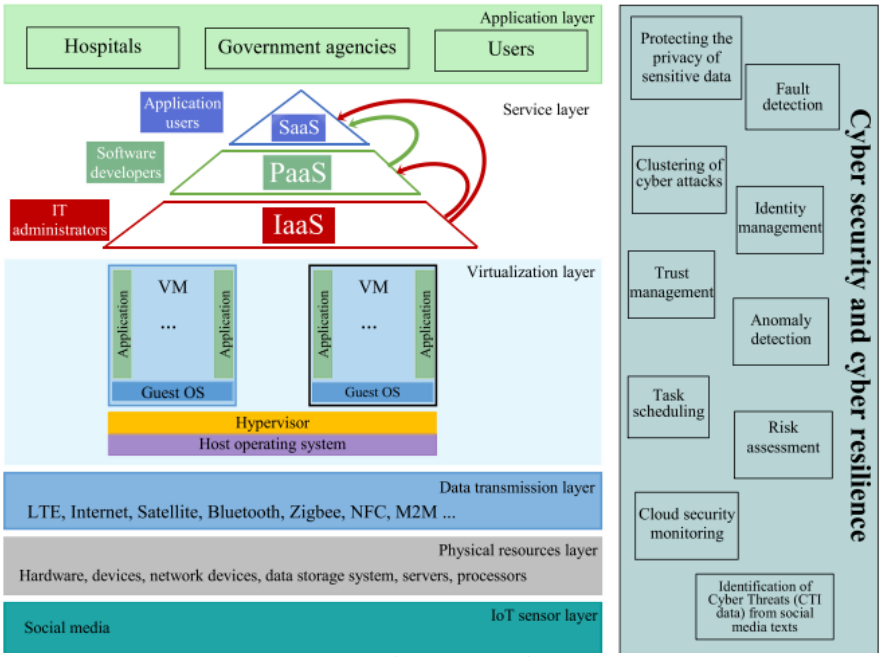

Fig. 3 The proposed cyber security reference model for the cloud computing system

3.3. Authentication Mechanisms

Through an authentication process, one entity verifies the authenticity of another, which is used to verify that a user or application is qualified to access or request data. Credentials, multi-factor authentication, third-party verification, clear-text passwords, 3D password objects, graphic passwords, biometric authentication, and digital device verification are commonly used online authentication methods. The cloud system may use any combination of authentication techniques [11]. Currently, the identity management system offers cloud access licensing.

3.4. Identity and Access Management Systems

Identity Management (IdM) functions include management, discovery maintenance, policy enforcement, administration, communication, and authentication. Identity and Access Management (IAM) authenticates and manages the same identity across applications and maintains security. The objective of it is to verify the authenticity of users, devices, and services while granting access to data and other system resources. The application can be accessed without needing additional identity storage or authentication methods from the system or service. Alternatively, authentication can be configured to use a trusted identity provider, which greatly reduces application workload.

Identity and access management facilitates the administration of large distributed systems. Identity and access rights management is used for business operations inside and outside the organization and between a private organization and a cloud service provider. IAM is primarily concerned with the organization of cloud objects and entities and resource management, which involves predetermined policies. The field of identity and access control consists of several functional areas. Management of entitlements, authentication, federated identities, compliance, and identity management and provisioning are functional areas.

Through these operational areas, efficient and secure access to the cloud is guaranteed for authorized users. XML serves as the base for the Service Provisioning Markup Language (SPML) identity management framework, allowing organizations to exchange information regarding users, resources, and services. SPML faces a drawback because it relies on vendor-specific protocols, resulting in diverse Application Interfaces (APIs). This variety complicates interaction among the APIs. The primary role of IAM is managing authentication.

It guarantees the secure management of credentials such as digital certificates and passwords. Third is unified identity management. The identity management service uses cloud services based on the specific identity provider your organization uses. Federated identity management ensures privacy, integrity, and non-repudiation. Public Key Infrastructure (PKI) authenticated public key exchange makes the web-based application and identity provider trustworthy. Licensing is the fourth field of activity. After successful authentication, rights management determines whether the authenticated entity is allowed to perform any actions in each application.

Compliance management represents the concluding aspect of identity and access management. It ensures the security and availability of the organization's resources following applicable policies and regulations. Identity management is critical to cloud security. The current approaches to identity management, particularly in public cloud environments, prioritize privacy and interoperability.

IAM systems are now useful risk mitigation tools in cloud environments. Organizations frequently implement IAM systems to safeguard information by controlling user access rights. IAM services are provided by renowned organizations such as SailPoint, IBM, Oracle, RSA, and Core Security. The management of passwords, compliance, data access rights, access requests, automation, and a single log are all features of the SailPoint identity management solution.

The IBM identity and access management product family provides solutions for web applications, user management, multi-factor authentication, enterprise single sign-on, privileged identity, user activity access control, and compliance. Oracle Identity and Access Management offers four cloud-based security options. Its products incorporate modern identity management techniques such as enterprise role handling, self-service account creation and maintenance, identity lifecycle management, and password management. Oracle IAM, which also supports identity federation, single sign-on, and privacy, provides another way to manage authentication and trust.

It also offers a third access control option that incorporates risk-based authorization, fine-grained permissions, and web services security in addition to directory services (virtual identities, persistent storage, and database user security), segregation of duties, compliance auditing and reporting, conflict management, function and architecture extraction, authentication, identity resolution and prevention, and fraud. Oracle IAM offers a Layer 4 identity and access control solution. Sync, fraud, etc.

Authentication, access control, identity management, risk analysis, and lifecycle management capabilities are all included in the RSA SecureID Suite. Core Security provides comprehensive solutions for managing identity and access control, encompassing password management and monitoring services. Different user accounts and account holder rights can be managed differently according to Privileged Identity Management (PIM). PIM creates identity management services and dedicated PIM products and processes. Popular PIM providers include Oracle PAM, CyberArk, and IBM PIM.

3.5. Multi-Factor Authentication (MFA)

An MFA is a method that validates if he or she possesses an identity associated with two or more factors before authorizing access to – for example, to an application or online account (via the VPN). MFA should be embedded in a sound Identity and Access Management (IAM) policy. By mandating the presence of one or more additional authentication elements alongside a username and password, MF can decrease the probability of surviving cyber attacks.

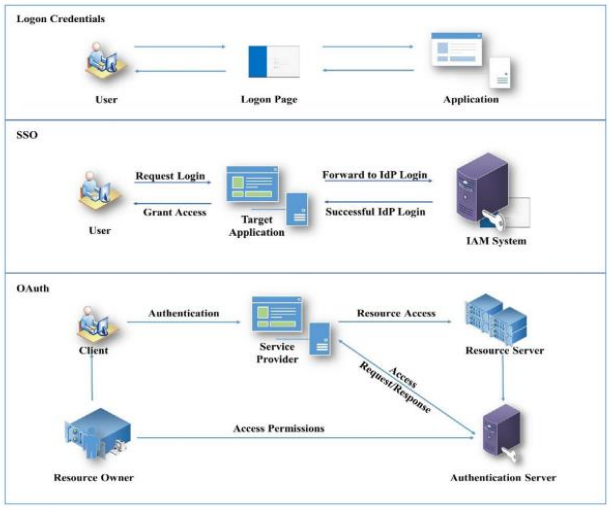

Fig. 4 Comparing authentication methods used in cloud computing

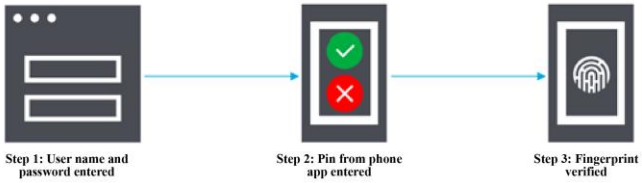

Fig. 5 Multi-factor authentication mechanism

3.6. Access Mechanism

Consider a scenario in which a user must sign in to an application and do so with multi-factor authentication and intrusion detection (see Figure 5, step 10). The following are the steps for the login script:

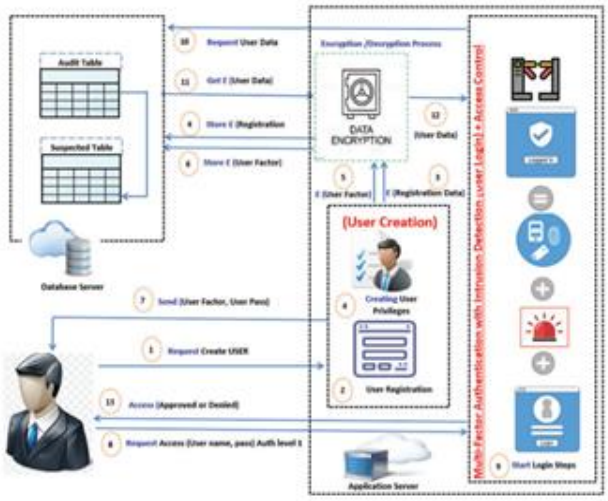

Fig. 6 Cloud security parameters

3.6.1. Level 1

As seen in Figure 7, the user enters his username and password for the first level of authentication. After verifying the encrypted username and password, the system sends a request to the database server to obtain roles and role access for the specified username.

The application server is subjected to Steps 1 and 2, as depicted in Figure 7. Steps 7 and 8 in Figure 7 involve decrypting and verifying access roles.

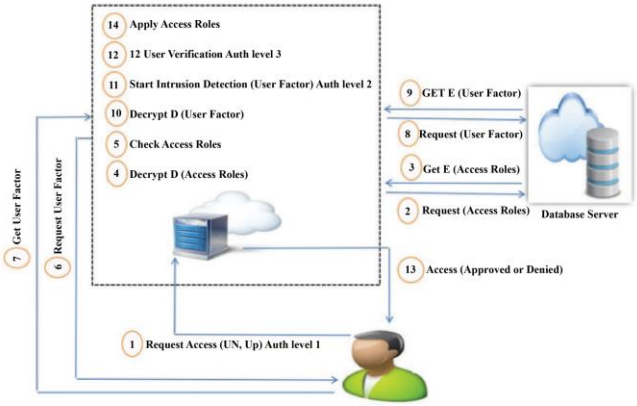

Fig. 7 Overall access mechanism

3.6.2. Level 2

The system requests user k to obtain a user access agent after verifying the username, password, and access roles, as illustrated in step 6 of Figure 7. Figure 8 displays the remaining steps. Once verified. Send a request to the server database to obtain the user access factor. As seen in Figure 7, steps 8 and 9, the encrypted user transmits the access agent to the application server. The user's access agent must then be decrypted (Figure 6, step 10). The procedures for intrusion detection evaluate the user access element from Step 7 by assessing its length, validity, and significance against the element presented in Step 10 of Figure 7. After that, the access factor is verified.

3.6.3. Level 3

At step 12 of Figure 7's representation, the user should obtain a confirmation message to enter the application. Figure 8 displays general access steps and intrusion detection procedures.

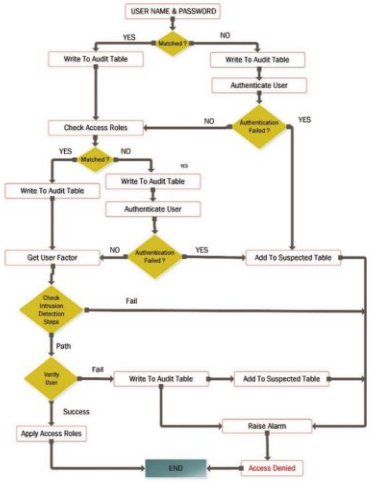

Fig. 8 General approach steps for intrusion detection

3.7. Intrusion Detection Steps

A 10-character system authentication factor has been suggested to prevent users from being hacked and entering different information lengths.

- Validation of factors: With an expired authentication factor, the user is unable to log in. A validity period (start and end dates) is associated with each user's authentication factor.
- The factor value should be compared to the following: The system verifies the provided factor against a saved user factor in the database to ensure its accuracy and a length of ten.
- Recheck the suspect table: Before granting users access to the application, make sure they do not already exist in the suspect table.

Figure 9 depicts the fundamental steps for intrusion detection.

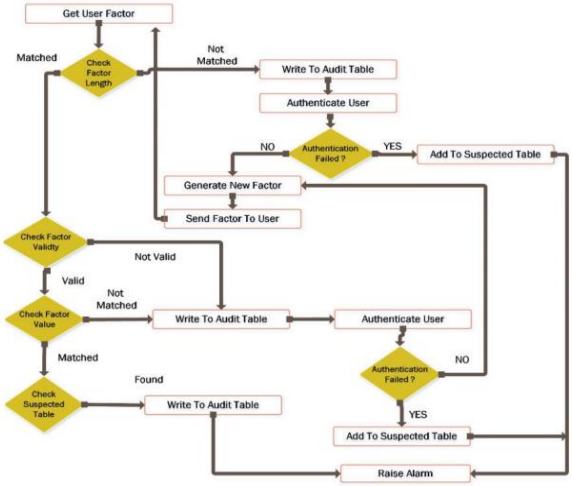

Fig. 9 Intrusion detection steps

3.8. Deep Learning

3.8.1. Distributed Denial-of-Service (DDoS)

DDoS attacks are currently destroying networks because they target crucial and sensitive cores. Additionally, DDoS attacks spread quickly, giving little opportunity for effective defense [22, 23]. In late 2018, Kaspersky Lab reported the emergence of new DDoS attackers such as Ox-booter. They utilize more than 16,000 compromised bots and bandwidth, reaching 420 Gbps. This platform is regarded as being extremely risky due to its simplicity of use and low cost. Using this straightforward interface, anyone can launch one of these attacks on a target for just $20 to $50.

3.8.2. DDoS Attack

Figure 11 illustrates various kinds of DDoS attacks. Three categories are typically used to categorize DDoS attacks: 1) Protocol-based attacks that use processing power or middle-layer resources crucial to the attacker's security to exploit a Layer 3 or Layer 4 vulnerability. 2) A target that might result in a service interruption, such as a firewall; and 3) application layer attacks, which involve convincingly communicating with the victim to explain the attack.

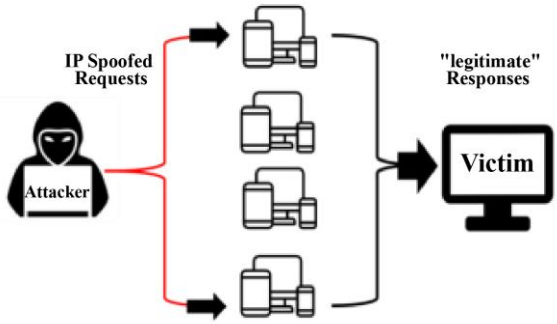

Fig. 10 DDoS attacks

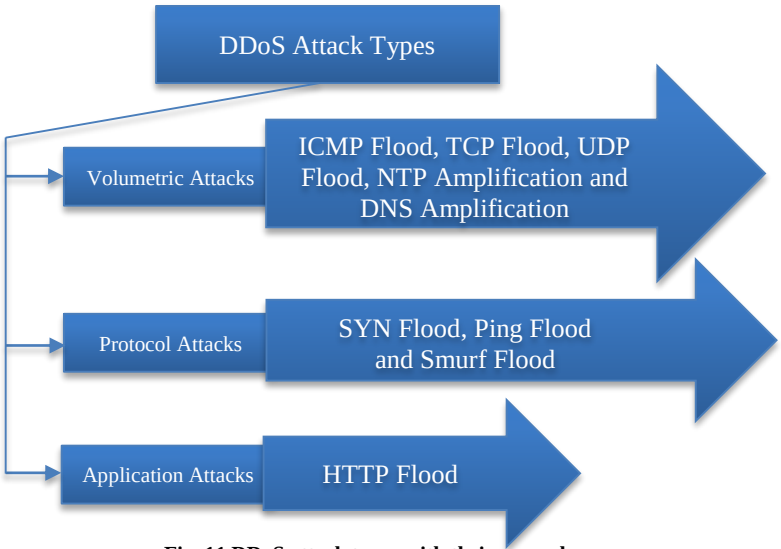

Fig. 11 DDoS attack types with their examples

Another tried-and-true method of detecting cyber-attacks with the security objectives of availability and integrity is an authentication-based solution. A straightforward cryptographic algorithm that can identify insertions is a potent tool for thwarting an attacker's attempt to maliciously insert false instructions or data into a server.

Attacks can also be discovered using honeypots and solutions based on intrusion detection. The distributed circuit breaker trips when the GOOSE protocol is attacked, turning off the power to the distribution system. Additionally, the electrical system tripped, failed, and tripped. Figure 12 illustrates how the electrical line behaves.

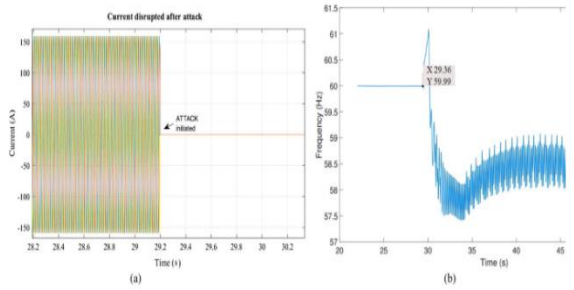

Fig. 12 Blackout after attack, (a) Current measurement, and (b) Frequency change.

3.8.3. Denial of Service Attacks

A denial-of-service attack is a straightforward and frequent attack targeting IoT devices. It prevents users from reaching services, applications, or data. An attacker must make requests to a target device, application, or service until it is unable to handle normal traffic to refuse service to other requesters. Figure 10 shows a denial-of-service attack in graphic form.

Attacks prompt cloud service providers to become less cautious, urging them to enhance their capacity to handle increased traffic and utilize additional resources while maintaining quality of service. In addition to being a cover for malicious activity that quickly spreads via cloud firewalls and brings down not just one device but many, denial-of-service assaults can also serve as catalysts. Consumers are unable to access computer services, such as cloud networks and the Internet of Things, due to Denial of Service (DoS) attacks.

A Denial of Service (DoS) attack on the Internet of Things (IoT) seeks to incapacitate a system and block user access. These assaults are difficult to identify, yet several strategies to combat them have been proposed.

Anti-Spoofing: To avoid dial-up spoofing, ensure that the IP address your traffic is coming from matches the address list of the website from which it came. Reduce transmissions: Attackers repeatedly send requests to all computers connected to the network to increase the attack. Attacks can occasionally be halted by restricting or halting transmission. Users can also disable the Charge and Echo services if necessary.

By optimizing the incident response time, your security team can quickly respond to DoS attacks. Make sure to patch any endpoints with known vulnerabilities.

It is necessary to install EDR agents on every endpoint. Firewalls should be installed to restrict both ingress and exit traffic.

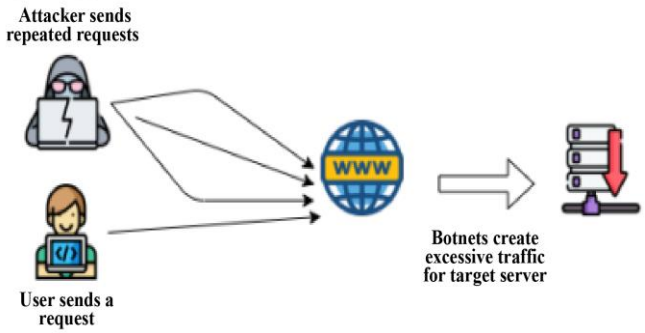

Fig. 13 Graphic of a denial-of-service attack

3.8.4. Malware Injection Attacks

An attacker employing a malware injection attack attempts to introduce harmful applications and services into the cloud. Keeping a view of the cloud model, the attacker uses multiple attack strategies. An attacker may create an instance of a malicious service application module or virtual machine and then attempt to upload it to the cloud. To execute malicious code, attackers attempt to depict this as a real-world scenario where they send legitimate user requests to the attacking service application.

A visual representation of a malware injection attack is shown in Figure 14. The attacker tried to access user resources and data using the cloud platform and manipulated the data. IoT is dependent on cloud computing because it is widely used and favored for storing data and resources on a global scale. One such attack uses the factory default login information to infect IoT devices with the Mirai malware.

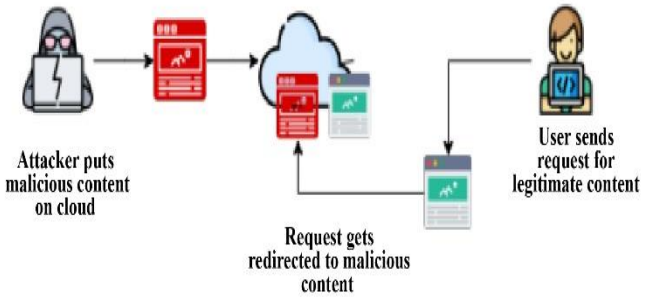

Fig. 14 Graphical representation of a malware injection attack

3.8.5. Botnet Attacks

Cybercriminals control a network of infected devices and execute extensive malicious operations during cloud attacks. Botnets spread by vigorously scanning a list of IP addresses in search of potentially dangerous hardware or network devices. The networks of users, businesses, and customers are seriously threatened by botnets. Spamming, Distributed Denial of Service (DDoS), data theft, and phishing attacks are among the malicious activities that botnets can carry out when they infiltrate a user's network. Their approach involves utilizing modern cloud computing platforms.

Additionally, using cloud services, a botnet expert can build botnets. Bot clouds, or cloud-based botnets, have quick internet connections and can continuously operate. Attackers utilize botnets to execute covert and challenging-to-stop attacks on their targets.

A graphic representation of the botnet attack is shown in Figure 14. Prevention is essential but challenging, given the current prevalence of botnets in the cloud. Botnets are constantly changing to exploit security flaws and vulnerabilities. Each botnet is, therefore, likely to differ greatly from the one before it.

To track accurate requests from clients and partners, IP addresses for attacks, and devices, bot operators ensure that their bot protection solutions regularly filter requests to their websites and APIs. This is challenging. Detecting and blocking bot attacks requires the use of advanced detection capabilities.

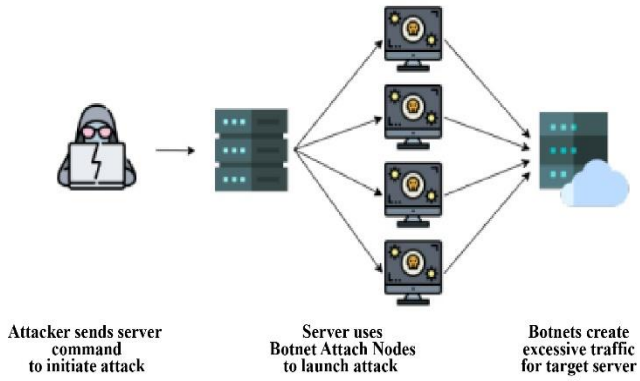

Fig. 15 A graph showing the operation of a botnet attack

This process entails the following four steps: The database is pre-processed before data from the project management module is extracted. Several algorithms are used to analyze and evaluate this pre-processed data, and after that, the estimated data is trained in a hybrid model. Based on the 80:20 learning model, the material was categorized into two sets: learning and testing. The output of the suggested algorithm for the hybrid model is shown in Figure 16.

3.9. Proposed DDoS Attack Detection Algorithm

Algorithm DDos Attack Detection: Hybrid Approach

1. Initialize:
   Import Python library file
   Import machine learning algorithms
   Import dataset
2. Data Processing:
   Sampling dataset, as 3000
   Remove empty values, item and dataset processing
3. Machine Learning Model:
   SVM(kernel = 'sigmoid', gamma = 'auto')
   Print (accuracy)
   Knn(n-neighbors=5)
4. Hybrid Model:
   Blanding SVM, KNN & GaussianNB
   [In]: Validation input and test input data
   [In]: Optimize with Random Forest Classifier
   print (model accuracy)

End
Output

Fig. 16 Proposed DDoS attack detection algorithm

Entropy determines the probability of an event compared to the total number of events. Low entropy values are regarded as test attacks that help determine the upper bound of entropy. The limit can be changed based on how the network is set up. Figure 17 depicts the virtual box opening the Mininet window.

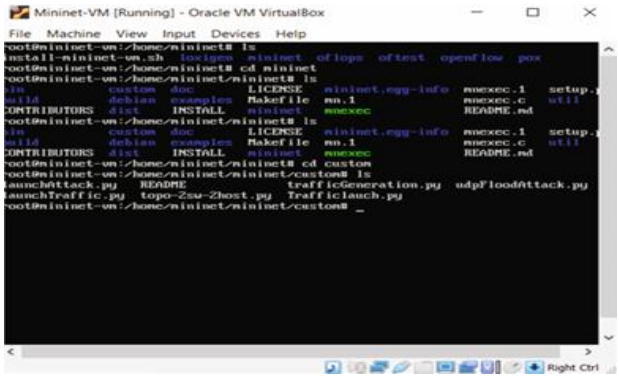

Fig. 17 Virtual box window running Mininet

4. Results

The suitability of the suggested design compared to current approaches using a variety of performance metrics. A typical metric for assessing the efficacy of IDS is the confusion matrix [5]. Acquiring crucial assessment metrics for model effectiveness. It emphasizes the significance of metrics such as precision, recall, and F1 score when evaluating deep learning DDoS detection techniques.

$$Accuracy = \frac{TP + TN}{(TP + TN + FP + FN)}$$

$$Precision = \frac{TP}{TP + FP}$$

$$Recall = \frac{TP}{TP + FN}$$

$$F1 - Score = \frac{2 \times Precision \times Recall}{(Precision + Recall)}$$

The Receiver Operating Characteristic Curve (ROC/AUC) graph illustrates the trade-off between a classifier's sensitivity and specificity. AUC values above a certain threshold indicate better prediction accuracy. The ROC for CyDDoS can be seen in Figure 18, where the x and y axes, respectively, stand for the false and correct classification rates. The diagram illustrates the proximity of the proposed solution to the optimal outcome, with true positives at one and false positives at zero. This demonstrates that 99.8% of DDoS and regular classes can be correctly classified by CyDDoS.

In general, exact recall curves assess a classifier's performance, particularly when the dataset is unbalanced. Measures of recall (completeness) and precision (relevance) are plotted on the x and y axes, respectively, and the trade-off between them is shown. A large area under the curve for CyDDoS, as seen in Figure 19, indicates that it performs well in both recall and precision. The average accuracy rate, shown as a red dotted line, is 0.999.

Figure 20 illustrates how the controller is typically used, so the controller only needs to compute the entropy value. Using this value, the controller can determine if the packet is an attack. Because there is no abrupt change in the entropy value that would suggest an attack, the controller does nothing.

The entropy number does not stay constant as it would in a stable environment when an assault is identified in the network in Figure 10. When the entropy value goes below a certain level (1 in this case), the threshold is met. One of the two hosts involved in the assault traffic in this instance was the target. The anticipated abrupt change in beam flux is depicted in Figure 21.

Figure 22 illustrates the comparison between the entropy values of normal traffic and attack traffic. As a result, when normal traffic increases above a certain threshold, the entropy value shifts and becomes apparent. The controller's detection of attack traffic and counting operations indicate that the entropy value is below the threshold. This leads us to conclude that entropy-based attack detection is efficient but less precise. In Figure 23, accuracy and f1-score show the comparisons.

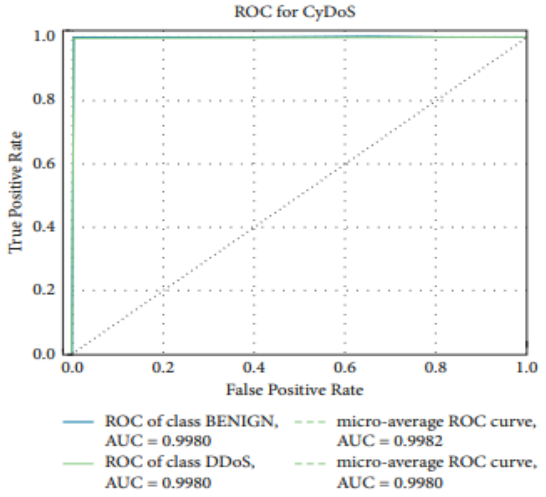

Fig. 18 ROC curve

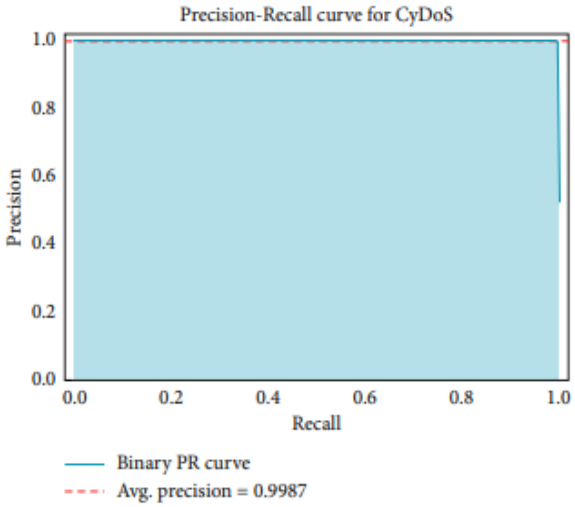

Fig. 19 Precision-recall curve

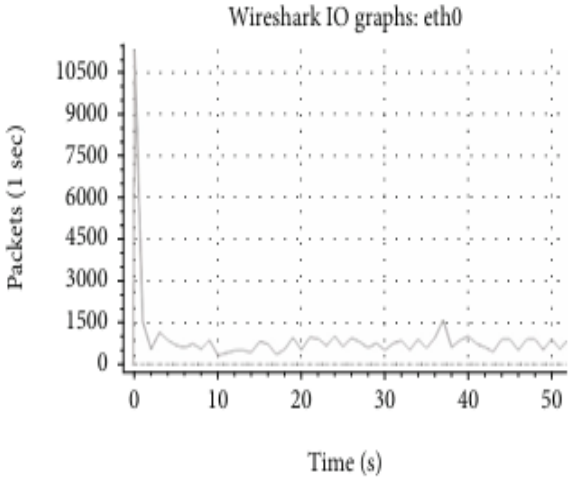

Fig. 20 The IO graphs of a typical host1 traffic exchange

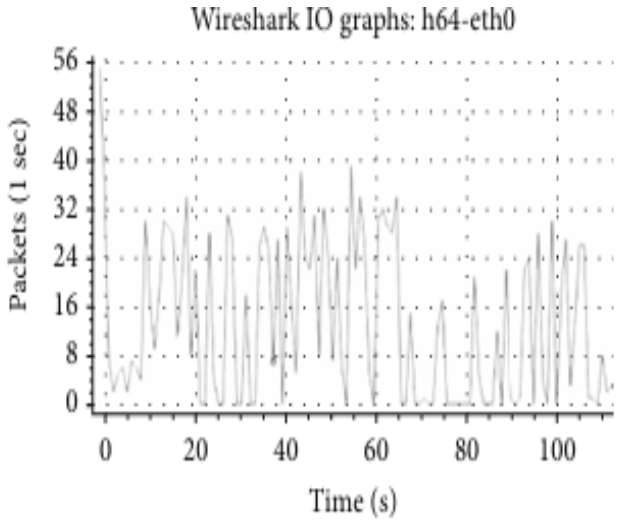

Fig. 21 IO graph of DDoS attack results of host 64

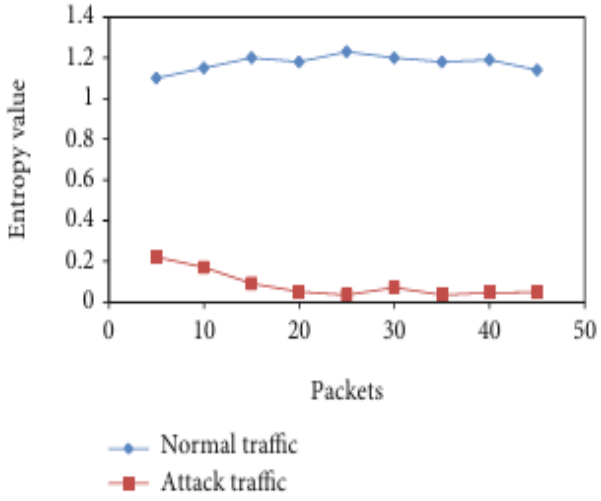

Fig. 22 The transformation of entropy leads to the development of normal and attack traffic

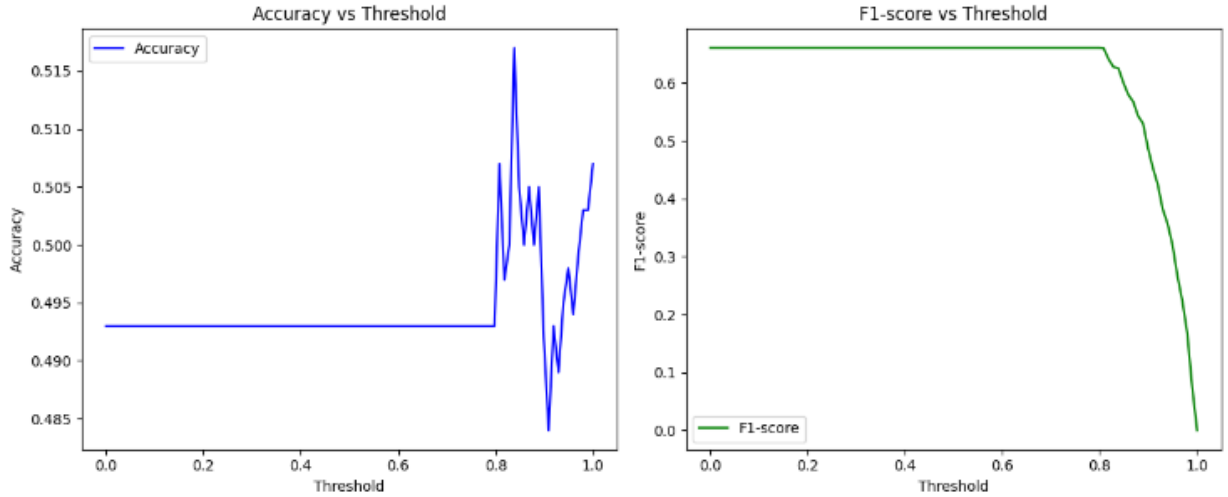

Fig. 23 Accuracy and F1-Score curve

4.1. Comparison with DL-Based Systems

The approach differs from existing machine learning techniques. It considers ROC, precision, recall, and F1 score. Table 1 unequivocally demonstrates that DDoS attacks outperform cutting-edge DL-based techniques in all metrics considered. It was created utilizing a Recurrent Neural Network (RNN) and an autoencoder. DDoSNet performs reasonably well compared to the model and is partially discussed regarding accuracy. DDoS, on the other hand, has a higher ROC rate of 1%. Because ROC represents classifier performance across the full spectrum of class distributions, it is the method of choice for comparing classifier performance.

Table 1. DDoS versus other deep learning models

Models	Accuracy	Precision	Recall	F1-Score	RoC
Kalman back Propagation NN	0.94	0.9122	0.9749	0.943	
Convolutional Neural Networks	0.954	0.933	0.924	0.928	
Meta-Classification / Decision Jungle	0.970	0.990	0.970	0.978	
DDoSNet	0.990	0.995	0.990	0.990	0.988
Proposed Model Over DDoS	0.996	0.997	0.997	0.996	0.998

Classifiers for both binary and multi-class tasks utilize decision forests. A decision forest, which serves as a meta-learning tool, combines the collective learning of many people to produce the best predictive performance. The accuracy of the proposed method is 0.99. A back-propagation Kalman neural network is proposed for DDoS detection in 5-G compatible IoT networks. The recall rating for this model was the highest (0.9749). The highest accuracy score, 0.954, was achieved by IDS based on convolutional neural networks.

5. Conclusion

This study suggested reference models to keep cloud systems' cyber security and resilience. The resulting attack classification uses the fundamental elements of the proposed model as its targets. They investigated the dangers, weaknesses, and risks of cloud computing. A common architecture has been created for intelligent cloud systems' security and resilience. The architecture includes functional elements that protect against different online threats. The intelligent cloud system can recover from unforeseen failures because these parts are created as separate clouds. A detailed explanation of the features and application scenarios for achieving a 'full solution' in multi-controller SDN architectures is provided in this article. Their strategy involves deploying a multi-controller SDN solution to prevent DDoS attacks on controllers. A logically centralized but physically decentralized POX console implements the environment. This provides several remedies for the drawbacks of a single console-based environment. In the early stages of a multi-controller architecture, DDoS attacks are successfully detected by this research. Finally, combine a model that more precisely and effectively detects and categorizes DDoS assaults in a multi-control SDN with an entropy-based deep learning approach. According to the test results, the accuracy of RNN was 98.6%, MLP was 98.3%, GRU was 96.4%, and LSTM was 99.42%. Among other suggested models, the LSTM demonstrated great accuracy. The combination of various machine learning algorithms. It discusses sophisticated methods such as transfer learning and interpretable AI, along with generative models and emerging fields like time series analysis and multi-modal learning.

References

[1] Abdul Basit et al., "Dynamic Event-Triggered Approach for Distributed State and Parameter Estimation over Networks Subjected to Deception Attacks," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 9, pp. 373-385, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[2] Lan Yao, and Xia Huang, "Memory-Based Adaptive Event-Triggered Secure Control of Markovian Jumping Neural Networks Suffering from Deception Attacks," *Science China Technological Sciences*, vol. 66, pp. 468-480, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[3] N. Ramana, and E. Hari Krishna, "Intrusion Detection System Fog Security Model for the Smart Cities and Urban Sensing," *Journal of Sensors, IoT & Health Sciences (JSIHS,ISSN: 2584-2560)*, vol. 1, no. 1, pp. 51-63, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[4] FIPS vs FedRAMP Compliance and Requirements, WolfSSL, 2024. [Online]. Available: https://www.wolfssl.com/fips-vs-fedramp-compliance-and-requirements/?utm_source=rss&utm_medium=rss&utm_campaign=fips-vs-fedramp-compliance-and-requirements&gad_source=1&gclid=EAIaIQobChMIx_egkOf5iwMVldAWBR2pMisrEAAYASAAEgIGTPD_BwE/

[5] EU Cloud Code of Conduct, Version 2.11, 2020. [Online]. Available: https://www.edpb.europa.eu/system/files/2024-02/eucloudcoc.pdf

[6] Jon Brodkin, Gartner: Seven Cloud-Computing Security Risks, Infoworld, 2008. [Online]. Available: https://www.infoworld.com/article/2174508/gartner-seven-cloud-computing-security-risks.html/

[7] Hanoch Levy, Eli Brosh, and Gil Zussman, Attack Resilient Resource Placement in Cloud Computing System and Power Grid, ICRC – Blavatnik Interdisciplinary Cyber Research Center, Tel Aviv University, 2023. [Online]. Available: https://en-cyber.tau.ac.il/research/Resilient-Resource/

[8] AKM Ahasan Habib et al., "False Data Injection Attack in Smart Grid Cyber Physical System: Issues, Challenges, and Future Direction," *Computers and Electrical Engineering*, vol. 107, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] Mohammad Kamrul Hasan et al., "Smart Grid Communication Networks for Electric Vehicles Empowering Distributed Energy Generation: Constraints, Challenges, and Recommendations," *Energies*, vol. 16, no. 3, pp. 1-20, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[10] Meenakshi Mittal, Krishan Kumar, and Sunny Behal, "Deep Learning Approaches for Detecting DDoS Attacks: A Systematic Review," *Soft Computing*, vol. 27, pp. 13039-13075, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] Mayadah A. Mohsin, and Ali H. Hamad, "Implementation of Entropy-Based DDoS Attack Detection Method in Different SDN Topologies," *American Scientific Research Journal for Engineering, Technology, and Sciences*, vol. 86, no. 1, pp. 63-76, 2022. [Google Scholar] [Publisher Link]

[12] Ankit Agarwal, Rajiv Singh, and Manju Khari, "Detection of DDOS Attack Using IDS Mechanism: A Review," *2022 1st International Conference on Informatics*, Noida, India, pp. 36-46, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Anshuman Singh, and Brij B. Gupta, "Distributed Denial-of-Service (DDoS) Attacks and Defense Mechanisms in Various Web-Enabled Computing Platforms: Issues, Challenges, and Future Research Directions," *International Journal on Semantic Web and Information Systems*, vol. 18, no. 1, pp. 1-43, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[14] S. Vijayarani Mohan, and S. Sharmila Sathyanathan, "Research in Cloud Computing-An Overview," *International Journal of Distributed and Cloud Computing*, vol. 3, no. 1, pp. 1-11, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[15] Ankit Agrawal et al., "Autoencoder for Design of Mitigation Model for DDOS Attacks via M-DBNN," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, pp. 1-14, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] Fatemeh Khoda Parast et al., "Cloud Computing Security: A Survey of Service-Based Models," *Computers & Security*, vol. 114, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[17] Tao Wang, Yaokai Feng, and Kouichi Sakurai, "Improving the Two-Stage Detection of Cyberattacks in SDN Environment Using Dynamic Thresholding," *2021 15th International Conference on Ubiquitous Information Management and Communication*, Seoul, Korea (South), pp. 1-7, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[18] Shanshan Yu et al., "A Cooperative DDoS Attack Detection Scheme Based on Entropy and Ensemble Learning in SDN," *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, no. 1, pp. 1-21, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[19] Omer Elsier Tayfour, and Muhammad Nadzir Marsono, "Collaborative Detection and Mitigation of DDoS in Software-Defined Networks," *The Journal of Supercomputing*, vol. 77, no. 11, pp. 13166-13190, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[20] Suhail Ahmad, and Ajaz Hussain Mir, "Scalability, Consistency, Reliability and Security in SDN Controllers: A Survey of Diverse SDN Controllers," *Journal of Network and Systems Management*, vol. 29, pp. 1-59, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[21] Yuanyuan Wei et al., "AE-MLP: A Hybrid Deep Learning Approach for DDoS Detection and Classification," *IEEE Access*, vol. 9, pp. 146810-146821, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[22] James Dzisi Gadze et al., "An Investigation into the Application of Deep Learning in the Detection and Mitigation of DDOS Attack on SDN Controllers," *Technologies*, vol. 9, no. 1, pp. 1-22, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[23] Ankit Agarwal, Manju Khari, and Rajiv Singh, "Detection of DDOS Attack Using Deep Learning Model in Cloud Storage Application," *Wireless Personal Communications*, vol. 127, pp. 419-439, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[24] Nisha Ahuja et al., "Automated DDOS Attack Detection in Software Defined Networking," *Journal of Network and Computer Applications*, vol. 187, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[25] Haomin Wang, and Wei Li, "DDosTC: A Transformer-Based Network Attack Detection Hybrid Mechanism in SDN," *Sensors*, vol. 21, no. 15, pp. 1-15, 2021. [CrossRef] [Google Scholar] [Publisher Link]