Adversarial Reinforcement Learning for Network Intrusion Detection in Fog Computing Environments

By
Seemab Ishfaq
1154-FOC/MSCS/F22

Supervisor
Dr. Qaisar Javaid

Department of Computer Science,
Faculty of Computing & Information Technology,
International Islamic University, Islamabad.
(2025)

Abstract

The abstract introduces a novel framework employing advanced machine learning techniques in fog computing environments. Generative Adversarial Networks (GANs) and Variational Autoencoders (VAEs) are used in this study's improved Intrusion Detection System (IDS) to boost threat detection. The suggested model achieves an 8-unit increase in accuracy over the conventional ESOMP-IDS framework when tested on the CICIDS2017 dataset. The method reduces false positives while efficiently detecting both known and unknown assaults by simulating typical network behavior. This makes it appropriate for vital industries including infrastructure, healthcare, and banking. However, the model has drawbacks. It may behave differently in various contexts and requires a lot of processing power to train. More research is also required to determine how resistant it is to adversarial attacks. Direct comparison with other IDS systems is also limited because some data are not shown as percentages. Notwithstanding these difficulties, the results demonstrate that deep learning methods can greatly improve IDS performance and provide a dependable defense against changing cybersecurity threats.

Table of Contents

List of Figures

List of Tables

Chapter 1: Introduction

1.1 Introduction

The emergence of cloud computing represents a major shift in the field of distributed computing and is redefining the boundaries between cloud infrastructure and edge networks. Unlike cloud computing, cloud computing brings financial applications closer to end users and supports real-time information and decision-making. Such a connection location has consequential advantages including low latency, efficient bandwidth, and enhanced security, the latter of which is relevant for IoT networks deployment. But, cloud computing accommodates a special architecture in the management of security. The possibility of a centralized control structure might be limited because the computing resources have to be dispersed to the various regions. More to it, limited air resources with low performance and storage capacity also call for safe and effective solutions. This has great security importance. These systems are normally designed based on static models which are not easy to accommodate to the behavior of the attack. Also, the complexity of the implemented NIDS models can be too high to be met by the limited resource availability, augmenting problems in deploying them and achieving high performance. There has also been an evolution in the network environment thus causing changes in the traditional NIDS changes and leaving cloud computing prone to threats. To solve these problems, this paper introduces a successful case for network access detection in a cloud environment with reinforcement learning named ARL. ARL has been developed to learn from both innocuous traffic and hostile ones; it is used for system protection to build stronger and more efficient detection strategies. Hence the proposed framework is very flexible. Fog nodes operate as data gatherers; they provide data from the network traffic while other data are pre-processed and features extracted at the central server. The main component of the framework is an ARL based NIDS agent which respectively interfaces with the network emulation of the central server [1].

An agent is trained continuously from two neural networks. the policy network, which classifies traffic as malicious or malicious, and the adversary network, which creates attacks and improves network policy to find capacity. Analyze different nodes for traffic distribution. It is done through the federated training system which assists in the perpetual alteration of threats

reciprocally whilst maintaining the confidentiality of the fog through the avoidance of data sharing and sharing of raw data. The subject of this paper is to show how indoor security can be enhanced when combining ARL and NIDS technologies to provide safety. Thus strategic planning and management allows for constan2t improvement and learning, resourcefulness and efficient exploitation, as well as advent security against new and changing threats to the environment. The future work includes the detailed analysis of various kinds of weather, the study of other ARL algorithms, and integration with security systems for enhancing the climate system [2].

Because cloud computing makes centralized, scalable, and effective resource management possible, it has drastically changed distributed computing. By decentralizing processing resources and placing them closer to end users and data sources, edge computing is altering this paradigm. By lowering latency and optimizing bandwidth, edge computing helps real-time applications such as IoT installations and financial services. In contrast to the conventional cloud approach, it does not need sending large volumes of data to centralized servers, allowing for quicker and more effective processing. One of the main benefits of edge computing is increased security. Edge systems reduce their vulnerability to possible cyberattacks during data transmission by processing sensitive data locally. Because of this, it is especially well-suited for Internet of Things networks, where real-time processing and anonymity are essential. Because edge computing is decentralized, security management is made more difficult. Because of the distributed nature of resources and operational limitations, centralized control structures which work well in cloud environments might not be practical in edge computing. Complex security model implementation is difficult due to edge devices' limited processing and storage capabilities. Lightweight and effective solutions that can function well under these resource limitations are required. Static models, which are frequently used in traditional security systems, are unable to keep up with changing cyber threats. Dynamic and adaptive security frameworks are essential for edge computing environments since this lack of flexibility raises vulnerabilities. In cybersecurity, Network Intrusion Detection Systems (NIDS) are essential. However, because of their high complexity, which surpasses the resource capabilities of edge devices, current NIDS models frequently fail in edge contexts [3].

This makes it more difficult to achieve strong security and great performance. Adaptive security models that make use of AI and machine learning are crucial for tackling these issues. By analyzing network activities, learning from new threats, and constantly modifying defenses, these models can provide strong security in real time. In edge computing, performance and security must be balanced. Some of the tactics being explored to successfully address this issue include integrated cloud-edge security systems, scalable authentication methods, and lightweight encryption. Cyberattacks on cyber-physical systems (CPSs) can result in safety hazards, significant physical object damage, and improper sensing and actuation behavior. Although machine learning algorithms have been developed to prevent cyberattacks on CPSs, it is difficult to identify these attacks due to the lack of labeled data from fresh attacks. Generative adversarial networks (GANs), which implicitly model the system, are a promising unsupervised method for detecting cyberattacks in this environment. However, because the assaults must be halted before the system is compromised, there are stringent latency requirements for the detection of cyberattacks on CPSs. We present FID-GAN, a new fog-based, unsupervised intrusion detection system (IDS) for CPSs that uses GANs, in this work [4].

1.2 Reinforcement Learning

A machine learning training technique called reinforcement learning (RL) teaches software to perform specific desired actions. Rewarding preferred behaviors and penalizing undesirable ones is the foundation of reinforcement learning. Machine learning systems are trained using a variety of techniques, including reinforcement learning. Because it enables an agent to learn how to negotiate the complexity of the environment for which it was designed, this method is significant. For instance, a robot in an industrial context can be trained to carry out a particular duty, or an agent might be trained to operate a video game. The agent gains knowledge from its surroundings and improves its actions over time with the help of a feedback system, which usually consists of incentives and penalties. The actions an RL agent does to move through its surroundings are called actions [5]. Choosing a tab to access a webpage is one example of this. Developers come up with a way to reward favorable behaviors and penalize undesirable ones in reinforcement learning. In this approach, undesirable behaviors are given negative values to deter the agent from engaging in them, while desired activities are given positive values to urge the agent to do so using a

reinforcement learning algorithm. In order to arrive at the best solution, this trains the agent to look for long-term and maximum overall rewards [6].

If there is a clear reward available, reinforcement learning can work. Reinforcement algorithms in enterprise resource management distribute scarce resources among various jobs as long as they are working toward a common objective. In this case, saving time or conserving resources would be an objective. Moreover, simulation-based optimization, multi-agent systems, swarm intelligence, statistics, genetic algorithms, operations research, information theory, game theory, control theory, and continuous industrial automation initiatives all make use of reinforcement learning. Over the past few years, the Internet of Things (IoT) has undergone substantial development, enabling the linking of numerous objects and enhancing data flow and communication. IoT has improved connectivity, efficiency, and comfort in many areas, making it a more essential part of modern life. IoT transforms the way we interact with our surroundings, by easily linking devices, sensors, and systems. Industrial control systems (ICSs), which link, monitor, and regulate physical processes in industrial settings including manufacturing, smart grid, smart transportation, and connected agriculture, are only one example of how technology has impacted users' daily life. By improving and refining services, IoT has created potential in telemedicine and healthcare. Because IoT devices are susceptible to several cyber threats, such as unlawful access and intrusion, this interconnectedness also raises serious security and privacy issues. Constantly connected devices are susceptible to hackers and require a flexible, real-time solution. Because of this, a lot of people have turned to RL to improve IoT security. Actually, in 2019, about 22% of businesses were already utilizing it. Devices can be protected by RL algorithms against jamming, malware injection, and eavesdropping. They can be used anywhere that a regular AI would be useful. They can, for instance, throttle incoming traffic in response to a distributed denial-of-service assault before it overwhelms the target servers. Since their method is a little difficult to duplicate, their real-world applications are extensive. Different learning strategies may be discovered by multiple models employed for the same job. However, because reward optimization drives their ongoing modification, they will still achieve the same end aim. The traffic-throttling algorithm will adapt until it finds a solution if it unexpectedly discovers that its strategy is ineffective. Because of their highly complicated learning style, RL models can have

a long calculation time, but the outcome is frequently worth it. They may react to a variety of situations and are quite dynamic [7].

As technology develops, IoT security is always changing, therefore an algorithm that can adapt is essential. Additionally, compared to other machine learning models, RL algorithms typically offer more notable advancements. In IoT security, they improve malware detection accuracy by 40%, whilst other solutions have a fixed success rate. primarily because their dynamic and realistic approaches provide original answers. The fact that RL can advance without assistance is one of the main reasons why people utilize it for IoT security. To learn, the agent does not require any prior knowledge of its surroundings. Finding realistic, pertinent, and reliable training data can be difficult, so this function is perfect. When researchers are unsure of what to train on to achieve their objective, they can utilize these models. IoT security requires a cutting-edge technology like RL. Its learning method and continuous reevaluation set it apart from other model versions that can adjust to fresh input. It doesn't need human assistance or prior knowledge to start training and execute its objective [8].

A subfield of machine learning called reinforcement learning (RL) focuses on teaching an agent to make decisions by interacting with its surroundings and picking up knowledge via trial and error. RL uses a reward-based system, in contrast to supervised learning, which trains models using labeled data. By acting in the environment and getting feedback in the form of rewards or penalties, the agent gains knowledge and is guided toward accomplishing its goal. Because of this paradigm, RL is especially well-suited for issues requiring sequential decision-making and flexibility. The agent (the learner or decision-maker), the environment (the system the agent interacts with), actions (the options the agent has), states (representations of the environment at a specific moment), and the reward signal (feedback based on the agent's actions) are the fundamental elements of reinforcement learning. In order to maximize cumulative rewards over time, the agent must create a policy, or strategy that associates states with actions. In order to approach optimal policies in complicated contexts, neural networks are used in techniques such as Q-learning and deep reinforcement learning.

The capacity of RL to manage intricate, changing, and unpredictable settings is one of its main advantages. It has been effectively used in a variety of fields, including robotics, where agents are trained to walk and manipulate things, and gaming, where RL algorithms have beaten human champions in games like StarCraft and Go. In real-world applications where judgments must be made instantly based on constantly shifting circumstances, such as driverless cars, personalized recommendations, and traffic control, reinforcement learning is also utilized. RL still faces a number of obstacles in spite of its achievements. Particularly in settings with sizable state and action spaces, training RL models can be computationally costly and time-consuming. Furthermore, creating suitable incentive signals is essential to guaranteeing that the agent picks up desired actions. Unintended consequences can result from poorly designed rewards, when the agent takes advantage of flaws in the system rather than resolving the intended issue. Another basic problem in reinforcement learning is striking a balance between exploitation (using known actions to maximize rewards) and exploration (doing new actions to collect more information). To sum up, reinforcement learning is an effective framework for resolving issues involving complex environments and sequential decision-making. Even though it has shown great promise in a number of fields, improving its application requires tackling issues with reward design, computational efficiency, and exploration tactics. RL has the potential to open up new avenues for automation and artificial intelligence as research advances [9].

1.2.1 Reinforcement Learning for Network Detection

An essential component of network security is network intrusion detection. Despite their strong detection performance, existing deep learning-based intrusion detection systems still struggle to identify unknown and minority threats and handle unbalanced datasets. In this work, we present the AE-SAC intrusion detection model, which is based on the soft actor-critic reinforcement learning algorithm and adversarial environment learning. In order to prevent, transfer, and lessen the risks that information systems face, intrusion detection technology uses an active defensive strategy that allows for timely and accurate warning before intrusions negatively affect computer systems. It also continuously builds a robust defense system. By continuously monitoring and analyzing network traffic, intruders are identified and dealt with promptly. Unquestionably, intrusion detection is essential to network security. Intrusion detection systems (IDS) are classified

into two categories based on intrusive behaviors: network-based intrusion detection systems and host-based intrusion detection systems (HIDS). For intrusion detection, DNN models are frequently used in conjunction with Convolutional Neural Networks (CNN), Gated Recurrent Units (GRU), Long-Term Short-Term Memory (LSTM), Deep Belief Networks (DBN), Stacked Auto encoders (SAE), and hybrid neural network models [10].

There are still a lot of issues to be resolved even though the use of deep learning in intrusion detection has produced the anticipated research results. On the one hand, the training dataset has a significant impact on deep learning models. However, the network intrusion detection data collected in the actual network environment frequently has a high proportion of data about normal behavior and a low proportion of data about attack behavior, making the dataset highly unbalanced. As a result, some incursions are not well recognized by deep learning models. However, creating high-quality models is really challenging. As everyone is aware, deep learning models have a large number of parameters, and fine-tuning them takes a lot of effort. Nomad detection is crucial for traffic classification and network security. Using machine learning and deep learning techniques, anomaly detection has been the subject of numerous studies aimed at enhancing network security. These techniques are limited in their versatility because they frequently call for a large number of samples and must classify the complete data set in order to get the desired results. The model's transferability has improved somewhat as a result of transfer and multitask learning, although these techniques need manual labeling or reprocessing of the test set. The use of earlier techniques in network security management is restricted by these issues [11]. We suggest a deep reinforcement learning-based transferable and adaptive network intrusion detection system (TA-NIDS) to address these issues. The interaction process between the agent and the environment varies every time. Numerous interactive processes can be generated from a small-scale data source. Consequently, when there are few samples, robustness is ensured. The agent can then learn how to select outliers without classifying the complete data set by using a fair reward mechanism. This increases the TA-NIDS's scene-adaptability when we give priority to apparent outliers. More significantly, the feature dimension is not needed because the initial characteristics are converted into the environmental state. Additionally, the model can be applied to various data sets because it captures the general rather than the unique condition of one data set [12].

Reinforcement Learning (RL) is becoming more and more recognized as a potent network detection method that provides clever and flexible answers to challenging cybersecurity problems. In order to detect malicious activity, intrusions, or unusual patterns in network traffic, network detection systems are essential. Conventional approaches use supervised learning models or preset rules that require labeled data, which can be hard to come by and might not generalize well to new threats. However, RL offers an adaptive method by interacting with the environment to learn the best detection algorithms, which makes it especially appropriate for dynamic and changing network settings. Fundamentally, reinforcement learning works by teaching an agent how to behave in a given environment in order to gradually increase a reward signal. Network traffic data makes up the environment in the context of network detection, and the agent's actions may involve putting defensive measures in place or flagging suspicious activity [13].

The reward signal is intended to show how well an agent has made decisions, such as correctly detecting threats while reducing false positives. In contrast to supervised learning, which necessitates labeled datasets, reinforcement learning (RL) makes use of trial-and-error learning, which allows the agent to enhance its performance in response to environmental feedback. The capacity of RL to function in dynamic and hostile environments is one of its main benefits in network detection. Because cybercriminals frequently modify their tactics to avoid detection, real-time adaptation in detection systems is essential. By constantly improving their detection policies, RL-based systems do exceptionally well in these kinds of settings. Particularly successful methods include Deep Q-Learning and Actor-Critic models, which combine deep learning and reinforcement learning to analyze massive amounts of network data and spot intricate patterns that point to hostile activity. Furthermore, by improving response plans and resource allocation, RL can raise the effectiveness of intrusion detection systems (IDS). For example, an RL agent can determine when to use computationally costly anomaly detection algorithms or prioritize which network packets to examine in-depth.

In large-scale networks with constrained computational resources, this is extremely advantageous. RL agents can enhance network detection systems' overall performance without sacrificing accuracy by learning how to distribute resources as efficiently as possible. Using RL for network discovery has drawbacks despite its benefits. High-stakes cybersecurity scenarios can make the exploration-exploitation trade-off where the agent must decide whether to adhere to known successful actions or try new ones particularly tricky [14].

Excessive exploration could result in ineffective functioning, while poor exploration techniques could expose the system to hidden hazards. A well-thought-out incentive system is also necessary for training RL models in order to prevent unwanted behaviors like overfitting to particular attack patterns. To sum up, reinforcement learning presents a viable path forward for network detection systems, offering flexibility and resilience in the face of changing threats. It is a desirable option for contemporary cybersecurity difficulties due to its capacity to learn from interactions and refine detection policies. To fully realize its potential, however, issues like exploratory tactics and processing efficiency must be resolved. RL has the potential to be a key component of next-generation network security systems with more study and development [15].

1.3 Problem Statement

A comprehensive Network Intrusion Detection System (NIDS) that can identify attacks in real time, adjust to new attack vectors, and preserve resilience in extremely dynamic infrastructures is urgently needed due to the growing complexity of cloud and fog computing environments. The static models that are frequently used in current NIDS systems are inflexible, have a significant computational overhead, and show little adaptability when dealing with distributed and resource-constrained settings, such as fog computing. Furthermore, the usefulness of present methods in recognizing new or complex threats is diminished since they usually fail to take advantage of insights from social and network activity.

1.4 Research Questions

1. Which ARL shall improve NIDS in fog computing, thus helping the process of learning and subsequently develop the defense strategy?

2. Some of the questions that deserve an explanation are associated with the fact that the ARL creates certain challenges for NIDS in fog computing context: scalability, amount of available resources, adversarial attacks, networks that have dynamic topology, and privacy/security issues.
3. Why use ARL for NIDS in fog computing to improve security in distributed systems as cyber threats shift to raise in complexity?

1.5 Research Objective

- Develop NIDS light for cloud nodes, prioritizing high efficiency and reduced resource consumption.
- Deploy federated learning in order to modify the central server network policy without necessarily disclosing the information, thus minimizing on communication.
- Increasing and decreasing metrics impacted against benchmarking data and climate metrics to find out framework effectiveness, accuracy and required means.
- Create the foundation of value-added decentralized network intrusion detection.

Chapter 2: Literature Review

2.1 Background Discussion

In reference [16], the authors introduce a novel intrusion detection method based on a reinforcement learning strategy specifically designed for adversarial environment. The paper is published in Computer Networks in 2019. In recent years, with the increasingly severe situation that modern cyber threats become more sophisticated in hiding malicious attacks or evading existing defense mechanisms, it becomes urgent to develop effective and adaptive intrusion detection systems. RL is a branch of ML from behavioral psychology. Reinforcement learning (RL) can enable an organism or intelligent machine to learn how to behave in an environment by performing certain actions and sensing feedback responses, such as rewards and punishments.
The authors consider the problem of network intrusion detection (NID) as a sequential decision-making process where an agent has the ability to sense environment states through observations and perform actions which have impacts on both observed states and future rewards. In particular, they apply RL techniques to train an autonomous NIDS agent that detects intrusions on-the-fly without any human intervention. Model evaluation experiments are conducted on common datasets. The results show that their proposed mechanism can detect most types of intrusion attacks with lower FP rates than previous works.' This work is expected to make contributions towards solving problems related to enhancing security against continuous threats over time.

In [17], the authors developed a novel architecture for intrusion detection systems (IDS) that integrates multi-agent systems with deep reinforcement learning.. Journal of Sensors and Actuator Networks 2023 method to improve IDS with the integration of deep reinforcement learning (DRL) technology together with generative models to enlarge the detection database. To tackle these constraints' issues, He introduce in this work a multi-agent IDS that uses DRL for optimizing his decision process. The proposed multi agent's architecture allows the use.

In [18], the authors proposed novel intrusion detection system (IDS) that is developed specifically for fog and edge computing environment. The paper has been published in Electronics in 2022. Recent development of Internet of Things (IoT)-based applications has paved the way toward the use of fog and edge computing technologies to enhance quality and latency requirements that could not be provided by using only cloud infrastructure. Nonetheless, with the

emergence of fog and edge computing challenging security issues associated with its decentralized architecture have been evolved as compared with those related to traditional centralized computing environments such as cloud systems along with conventional IoT networks due to their distributed nature. To overcome this issue using machine learning-based algorithms are introduced aiming at improving accuracy and efficiency of IDS mechanisms within dynamic computers environment such as fog and edge ones. By conducting optimization process, which depend on several settings into IDS, it attains considerable enhancement performances which reflect on improving several performance evaluation metrics. then they made extensive evaluations towards their obtained optimized ML- based IDS system . In these experiments, they reported high level results using the obtained experimental results clearly demonstrating that proposed model enhanced overall performance evaluations metrics over earlier models while achieved highly accuracy result beside reducing false positive rate"

In [19] , the authors introduce a new intrusion detection approach tailored for fog computing, For this purpose, a hybrid methodology that combines auto encoder and isolation forest models is proposed to detect anomalies in fog computing systems. Auto encoders are used for feature extraction and dimension reduction, and isolation forests are used for anomaly detection. The experiment results show the effectiveness of their hybrid model to better detect intrusions with minimum false-positive rates. Receive date: August 8, 2020; acceptance date: August 18, 2020; publication date: September 9, 2020; current version published online: September 23, 2020. The main goal of this study is to enhance the intrusion detection ability over fog computing to secure decentralized infrastructure.

In [20], the authors propose a novel model specifically designed for the (IOT) environments using a hybrid cloud-fog computing architecture. Published in the Security and Communication Networks journal in 2023, the study focuses on developing a lightweight intrusion detection model to mitigate these risks. The proposed model, ConvNeXt-Sf, leverages a modified version of the ConvNeXt computer vision model, adapted for IoT intrusion detection. By reducing the model's dimensionality and incorporating design criteria from the lightweight computer vision model ShufeNet V2, ConvNeXt-Sf achieves significant improvements in efficiency without compromising detection capabilities. The study evaluates the model using TON-IoT and BoT-IoT

datasets, demonstrating that ConvNeXt-Sf outperforms traditional models in terms of accuracy and false acceptance rate (FAR). Specifically, compared to ConvNeXt, ConvNeXt-Sf reduces training and prediction times by 82.63% and 56.48%, respectively, while maintaining or even enhancing learning and detection capabilities. Additionally, ConvNeXt-Sf achieves a 6.18% increase in accuracy and a 4.49% decrease in FAR compared to traditional models. The research underscores the effectiveness of ConvNeXt-Sf in addressing the lightweight intrusion detection requirements of fog computing in IoT environments, thereby enhancing information security in cloud-fog hybrid architectures.

In [21], the authors introduce a novel method for improving irrigation systems via deep learning based anomaly detection. Published in the journal Sensors 2024, the work introduces a smart and sustainable irrigation system that is capable of detecting water distribution network anomalies using deep learning. The authors utilize deep learning techniques to process data collected by sensors placed at different points in the network in order to identify leaks or blockages on the network. The low cost of both the sensors and their installation paired with the power of input data processing using deep learning models make this approach more accessible compared to existing efforts with similar goals. The authors demonstrate how their innovative approach significantly reduces water loss resulting from increased water efficiency within current agricultural irrigation practices. The following table presents an overview of key results achieved after evaluating this innovative irrigation system.

In [18], the authors proposed in this article capable of adaptively learning and enhancing its detection capabilities with the help of deep reinforcement learning algorithms. Performance analysis on different performance parameters has been performed to verify the finest performance of IDS showing noteworthy accurate intrusion recognition along with reduced false positive alarms. Table summarizes key results obtained by evaluating IDS which helps to detection accurately.

In [22], the paper proposed intrusion detection system. We published our research in Wireless Communications and Mobile Computing, Volume 2022 where we discussed why it is essential to have a reliable cybersecurity mechanism in Industry. The IDS employs DRL algorithms that utilize Q-learning along with an experience replay mechanism for efficient decision making. In particular,

our IDS can adaptively learn and enhance its performance over time as well as identify and mitigate effectively different cyber threats using DRL techniques. The obtained results demonstrate that our proposed IDS outperforms traditional machine learning-based IDS methods in terms of higher accuracy rate while maintaining reduced false-positive rates.

In [23], the paper addresses the need novel anomaly detection approach in fog computing architectures targeted for IoT based environments. He present a custom Tab Transformer model that can analyze data streams generated by IoT devices and identify abnormal patterns to detect potential security threats or system failures. Moreover, we exploit the superior aspects of the Tab Transformer architecture to achieve high-accuracy anomaly detection with minimal computational overhead in resource-constraint fog computing environments. We evaluate our proposed custom Tab Transformer on multiple benchmark datasets and demonstrate its improved anomaly detection performance over traditional models.

In [23], The authors address the problem of network intrusion detection in distributed scenarios while preventing data exposure among participant's nodes as much as possible. The proposed F-NIDS (Federated Network Intrusion Detection System) applies federated learning to perform joint training of local network nodes' models without information exchanges with a central server. We enhanced the scalability and privacy aspects associated to an intrusion detection system by making it conceivable that local models are trained over local dataset samples which constitute a fraction of global collected samples related to all participant's nodes in the collaborative scenario. In this paper F-NIDS was evaluated using published datasets which proved that the Complexity (in terms of training time), False Negatives Rates and False Positives Rates presented improvements regarding state-of-the-art studies in private no collaborative environments related works.

2.2 Reinforcement Learning and Network Detection Scenario

In [24] Multi-agent reinforcement learning models for intrusion detection in Internet of Things networks are investigated in this paper. In order to maximize the state-action mappings, it suggests a novel architecture and emphasizes the usage of a hierarchical system that detects anomalies. The study highlights the difficulties of non-adversarial agent interactions in large-scale networks and highlights how flexible reinforcement learning is in various IoT contexts. Additionally, it presents

new datasets and emphasizes how crucial real-time adaptation is in fog computing scenarios. Malicious actors have found Internet of Things (IoT) systems to be appealing targets due to their growing popularity. Finding and creating new algorithms that are quick and reliable in identifying and categorizing harmful network traffic is crucial in order to handle the changing threats and the increasing complexity of detection. Because it allows autonomous agents to collaborate with their surroundings for decision-making without depending on human specialists, deep reinforcement learning (DRL) is becoming more and more recognized as a potential solution in many domains. In this paper, an adversarial reinforcement learning (RL) algorithm with remarkable predictive power is used to introduce a novel method for intrusion detection in Internet of Things systems. The classifier, which is a simplified and incredibly effective neural network, is the foundation of the prediction process. This classifier incorporates a policy function that was painstakingly learned using a cutting-edge RL model. Crucially, this model guarantees that the behavior of the environment is dynamically adjusted concurrently with the learning process, enhancing the intrusion detection method's overall efficacy. The Bot-IoT database, which combines simulated attack scenarios with real-world IoT network traffic, was used to evaluate the effectiveness of our proposal. Our system performs better than others that are currently in use. As a result, our method for IoT intrusion detection can be regarded as a useful substitute for current techniques, capable of greatly enhancing the security of IoT systems. The Internet of Things (IoT), a paradigm in which common objects are connected through information-sensing devices to promote information sharing, has emerged in large part due to the Internet's rapid development. Connecting various objects to the Internet so they can communicate with one another is the goal of the Internet of Things. Applications like smart cities, smart homes, and healthcare systems where intelligent identification and management are achieved have emerged as a result of this connectivity. Like any widely used technology, IoT has drawn the attention of cybercriminals who aim to exploit its flaws by employing advanced hacking methods like botnets. Security issues have been made worse by the proliferation of low-cost, lightweight, and energy-efficient devices as well as the lack of standards in IoT systems.

In [25]Using a trial-and-error framework, this paper suggests a Deep Q-Learning (DQL) method for network intrusion detection. It focuses on a continually learning, self-updating platform

that adapts to quickly changing cyber threats. By adjusting hyperparameters such as discount factors and testing the model on the NSL-KDD dataset, the study outperforms conventional machine learning techniques. It emphasizes how crucial it is to keep learning in order to adjust to hostile surroundings and zero-day attacks. More advanced and intelligent cyber protection solutions with autonomous agents that can learn to make judgments without the assistance of human specialists are required due to the emergence of the new generation of cyber threats. In recent years, a number of reinforcement learning techniques (like Markov) have been put out for automated network infiltration jobs. In this study, we provide a novel approach to network intrusion detection that combines a deep feed forward neural network technique with reinforcement learning based on Q-learning. Our suggested Deep Q-Learning (DQL) model offers a network environment continuous auto-learning capability that can identify various network intrusion types through an automated trial-error method and continually improve its detection skills. We offer the specifics of adjusting the various DQL model hyperparameters for improved self-learning. Our extensive experimental results on the NSL-KDD dataset demonstrate that the greatest performance outcomes are obtained with a lower discount factor set at 0.001 under 250 training episodes.

Our experimental findings also demonstrate that our suggested DQL works better than other comparable machine learning techniques and is very successful in identifying various intrusion classes. Reinforcement Learning (RL) has gained popularity as a method for deploying automated agents to detect and categorize various threats. The agent creates a defense plan to better safeguard the environment going forward by learning the various behaviors of attacks made against particular settings. By rewarding or penalizing an action after obtaining input from the environment, an RL technique can enhance its capacity to preserve the environment (e.g., in a trial-and-error interaction to find what works better with a certain environment). Over time, an RL agent can improve its capabilities. Unfortunately, the majority of current methods struggle to accurately identify valid network traffic and are unable to handle big datasets. This is because an RL agent would run into the state explosion issue when dealing with very large learning states. The primary limitation of current reinforcement learning (RL) techniques has been addressed in recent years by the proposal of deep reinforcement learning (DRL) techniques, which can learn in an environment with an

unmanageable large number of states. By utilizing deep neural networks throughout the learning process, DRL approaches like deep Q-learning have proven to be a viable way to address the state explosion issue.

In [26] This study explores the difficulties associated with fog nodes' constrained processing capabilities when creating an intrusion detection system (IDS). The work classifies incursions in contexts with limited resources by combining feature optimization and machine learning. It draws attention to the particular weaknesses of fog computing and offers benchmarks based on real-time datasets. One computing paradigm that operates Internet of Things (IoT) applications at the network's edge is fog computing (FC). Data demands and FC have increased significantly in recent years, which has improved data accessibility and adaptability. Nevertheless, FC has encountered numerous difficulties, such as load balancing (LB) and failure adaption. Although numerous LB techniques have been put out for cloud computing, they have yet to be successfully implemented in fog. Achieving high resource utilization, avoiding bottlenecks, avoiding overload and low load, and decreasing response time are all made possible by LB. This research proposes a dynamic resource allocation method based on reinforcement learning and genetic algorithms for LB and optimization strategy (LBOS). LBOS continuously monitors network traffic, gathers data about server load, responds to incoming requests, and uses the dynamic resource allocation mechanism to divide them evenly across the available servers. As a result, it improves performance even during peak hours. Thus, in real-time fog computing systems, like the healthcare system, LBOS is easy to use and effective. LBOS is focused on creating a healthcare system that is built on IoT fog. Ultimately, the tests are conducted, and the findings demonstrate that the suggested method lowers reaction time and enhances quality-of-service in the cloud/fog computing environment in terms of allocation cost. The LBOS attained the best load balancing level (85.71%) when compared to the most advanced algorithms. As a result, LBOS is a productive method for determining resource usage and guaranteeing uninterrupted service.

In [27] An adversarial agent creates misleading attacks during the training phase of the reinforcement learning system presented in this paper. This method makes IDS more resilient to actual attack situations. The paper shows enhanced resilience against adversarial perturbations in fog and IoT networks using datasets such as NSL-KDD. Recent advances in reinforcement

learning (RL) have been made possible by deep neural networks, quick simulation, and faster computing speeds. However, the majority of existing RL-based methods are unable to generalize because: (a) the gap between simulation and the real world is so great that policy-learning methods are unable to transfer; and (b) even when policy learning is conducted in the real world, the lack of data results in unsuccessful generalization from training to test scenarios (for example, because of different object masses or friction). We observe that modeling errors and variations between training and test scenarios can simply be seen as additional forces or disturbances in the system, drawing inspiration from H-infinity control techniques. In order to train an agent to function in the presence of a destabilizing opponent that imparts disturbance forces to the system, this study introduces the concept of resilient adversarial reinforcement learning (RARL). By learning an optimal destabilizing policy, the adversary that has been jointly taught is strengthened. The policy learning is formulated as a minimax, zero-sum objective function. Inverted Pendulum, Half Cheetah, Swimmer, Hopper, Walker2d, and Ant are just a few of the environments in which extensive experiments show that our method (a) enhances training stability; (b) is resilient to variations in training/test conditions; and (c) outperforms the baseline even when the adversary is not present. Learning a policy that is resilient to simulation modeling errors or mismatches between training and test scenarios is our aim. For instance, we want to understand the Walker2D strategy that applies to walking on ice (test scenario) as well as carpet (training scenario). Likewise, throughout training and testing, other variables, including the walker's mass, may change. Listing every one of these characteristics (mass, friction, etc.) is one option.

In [28] The study introduces a deep reinforcement learning-based distributed monitoring system for Internet of Things networks. In adaptive environments, agents work together to identify and stop various attack types, increasing the overall resilience of the system. The strategy is appropriate for dynamic IoT environments since the introduction of adversarial scenarios increases the agents' learning robustness. Federated Learning (FL) is a distributed machine learning framework that aims to maintain device data privacy by exchanging local model parameters between devices and a centralized server without disclosing the actual data. The Hierarchical Federated Learning (HFL) framework was developed to increase the effectiveness of FL communication in situations when devices are grouped together and use edge servers (such as base

stations) to seek model consensus. At each iteration, devices in a cluster send their local model updates to the designated local edge server for aggregation. The edge servers create a worldwide consensus and send the combined models to a centralized server. But just with FL, enemies could jeopardize HFL's privacy and security. By using poisoning attacks or poor-quality model updates brought on by erratic communication channels, increased device mobility, or insufficient device resources, client devices in a cluster may purposefully offer unreliable local model updates. This study examines the client selection issue in the HFL framework to mitigate the effects of untrustworthy clients while optimizing the global model accuracy of HFL in order to overcome the aforementioned difficulties. A reputation model based on Deep Reinforcement Learning (DRL) is installed on each FL edge server to quantify the dependability and credibility of FL workers in its cluster as accurately as possible. Given the dynamic behaviors of the workers in the HFL environment, a Multi-Agent Deep Deterministic Policy Gradient (MADDPG) is used to improve the accuracy and stability of the HFL global model. According to the experimental findings, our suggested MADDPG outperforms the single-agent DDPG-based reputation model and the traditional reputation model in terms of accuracy and stability of HFL.

2.3 Fog Computing

In [29] Auto encoders are used in this study to detect intrusions in fog networks. Decentralized learning is made possible via fog nodes, which also increase scalability and lower latency. It compares auto encoder-based deep learning models with shallow architectures using NSL-KDD datasets, demonstrating notable improvements in accuracy. Fog Computing has arisen as an extension to cloud computing by offering an effective infrastructure to serve IoT. By serving as a mediator, fog computing reduces communication delays between end users and the cloud through fog devices and processes end users' requests locally. As a result, it is crucial that incoming network traffic on the fog devices be legitimate. These gadgets are susceptible to malevolent assaults. These devices carry a wide range of data, particularly financial and health data. Attackers send malicious data packets to these devices in order to target them. To give the consumer a safe and dependable service, it is essential to identify these invasions. For fog to operate safely without sacrificing effectiveness, an intrusion detection system (IDS) must be strong. In this work, we provide Auto-IF, a deep learning-based intrusion detection system that uses Auto encoder (AE)

and Isolation Forest (IF) for fog environments. Since fog devices are more concerned with instantly distinguishing attacks from legitimate packets, our method solely focuses on binary classification of incoming packets. We use the benchmark NSL-KDD dataset to validate the suggested approach. Compared to many other state-of-the-art intrusion detection techniques, ours obtains a high accuracy rate of 95.4%. IoT gadgets, such as smart cars, gaming, banking, home alarm systems, and health monitoring systems, need the right environment. High latency, high energy consumption, intrusion detection, secure communication, etc. have become important challenges as IoT devices for real-time applications proliferate. The issues of cloud computing's high latency and high energy consumption have been addressed via fog computing. Fog computing, a term coined by Cisco to describe comprehensive cloud computing, often referred to as edge computing or fogging, makes it easier to conduct computer operations, store data, and provide networking services among fog devices, cloud center data storage devices, and end devices. The authors provide a thorough analysis of the differences in energy consumption and latency (communication delay) between cloud and fog computing. Effective and efficient security elements are installed in the cloud data centers and other cloud processing units. However, the fog devices are susceptible to attacks by malevolent entities on the network due to their low CPU, memory, and other resource levels. To damage user data, an intruder or attacker could get into the network. An effective method for identifying network intrusions is an intrusion detection system (IDS).

In [30] In order to identify irregularities in IoT networks, the study combines deep belief networks with deep learning frameworks. Using real-world smart home datasets, it tests its methodology and demonstrates excellent precision and recall against intrusion attempts. Robustness is ensured throughout training by utilizing adversarial approaches. Since the emergence of the Internet of Things (IoT), there has been an increasing focus on network layer security. The intricate Internet environment of the Internet of Things makes it impossible for typical intrusion detection solutions to function effectively. A neural network structure may have fine detection accuracy for one type of attack in the deep learning intrusion detection technique, but it may not have a good detection effect for other types of attacks. Designing a self-adaptive model to modify the network structure for various assault types is therefore crucial. An intrusion detection model based on deep belief networks (DBN) and enhanced genetic algorithms (GA) is

presented in this research. In order for the intrusion detection model based on the DBN to achieve a high detection rate with a compact structure, the ideal number of hidden layers and the number of neurons in each layer are adaptively created through numerous iterations of the GA in response to various attack types. Lastly, the model and methods were evaluated and simulated using the NSL-KDD dataset. The experimental findings demonstrate that the enhanced intrusion detection model in conjunction with DBN can successfully raise the intrusion assault identification rate while lowering the neural network structure's complexity. A network structure may have a high detection accuracy for one form of attack for the deep learning algorithm, but it may not have a strong detection effect for other types of attacks. In order for our intrusion detection model to consistently maintain a high detection rate, we therefore intend to create a self-adaptive model that can modify the neural network topology for various assault types.

In [31] His research centers on integrating adversarial training into deep reinforcement learning for intrusion detection systems. The technology detects and counteracts assaults that target known weaknesses in fog networks. Adversarial examples simulate actual assault scenarios, increasing the model's resilience. Due to the growing threat of cyberattacks on critical infrastructure networks and distributed devices, anomaly detection is one of the most significant security concerns in the Industrial Internet of Things (IIoT). The Intrusion Detection System (IDS), a strong tool for guarding against and keeping an eye on hostile activity in IIoT networks, is recommended as a solution to these problems. In this study, we propose a novel technique that uses the Generative Adversarial Network (GAN) and Distributional Reinforcement Learning (DRL) to increase the robustness and efficiency of the IDS system. To address the problem of data imbalance, we use manufactured data to create a realistic and balanced distribution for a particular feature set. We demonstrate how the GAN can effectively support the distributional RL-based-IDS in improving minority attack detection. We used the Distributed Smart Space Orchestration System (DS2OS) dataset to test the efficacy of our algorithm and evaluate the taxonomy of our method. On the basis of anomaly detection datasets, the normal DRL and DRL-GAN models' performance in binary and multiclass classifications was assessed. In the usual criteria of accuracy, precision, recall, and F1 score, the suggested models fared better than the typical DRL. We showed that the greatest results are obtained when a GAN is included to the DRL training process in order to enhance the detection

of a particular type of data. The sensor, which gathers data and transmits it to the central agency for additional processing, is a crucial component of the Internet of Things environment. Through the internet, the smart devices communicate with one another and share information. By utilizing sensors, smart environments seek to enhance human well-being while also boosting environmental efficiency. The term "Industrial Internet of Things" (IIoT) refers to the application of traditional Internet of Things concepts in industrial settings. IIoT improves production by making it possible to employ efficient and sustainable technology in an industrial setting. The IIoT industry is currently expanding quickly and becoming more adaptable as a result of numerous sectors' digital changes. Because of the strong partnerships and shared interests among IIoT players, major corporations from all over the world are investing in this developing market. Due to the new applications, the market has drawn big businesses from all over the world. Security is a major issue for IIoT systems due to the increasing number of clients and departments using these systems.

In [32]In order to prevent DDoS attacks, this study creates a lightweight intrusion detection system for fog-based IoT networks. For high detection accuracy, it combines deep learning classifiers with sophisticated preprocessing methods. BoT-IoT and other large-scale datasets are used to benchmark the model. In the current digital era, distributed denial of service (DDoS) assaults are becoming more common, especially as the number of unprotected Internet of Things (IoT) devices increases. The rise in attacks calls for the creation of adaptive intrusion detection systems (IDS) that are effective at detecting threats and need fewer resources, making them appropriate for Internet of Things devices with limited resources. The most common methodology for creating effective and lightweight IDS is feature selection (FS). However, because of the inherent bias in datasets, FS approaches must be varied and flexible. By combining the best features of seven distinct filter-based techniques, this research suggests a novel Ensemble FS method called Ensemble Feature Selection for Lightweight IDS (ELIDS). In addition to reducing features, ELIDS converges the selection process on the most important features among those found by the various FS techniques. Robust classification models are constructed using ELIDS, taking into account several learning techniques, and thoroughly assessed for performance and resumption using both in-domain and cross-domain testing. Results from in-domain testing show that classification models constructed using ELIDS typically have accuracy levels comparable to those

constructed using the current individual FS approaches, with high accuracy rates of 99.8% attained. Cross-domain testing, however, shows that classifiers constructed using individual FS methods exhibit a noticeable decline in accuracy, while the suggested ELIDS demonstrate robustness by significantly surpassing current methods. In fact, when using Random Forest (RF) as the learning method, ELIDS outperforms current solutions by at least 23.7% in terms of accuracy. Due in large part to the proliferation of unprotected Internet of Things (IoT) devices, distributed denial of service (DDoS) assaults are becoming more common in today's digital world. Because of this increase in attacks, adaptive intrusion detection systems (IDS) that are effective at detecting threats and require fewer resources must be developed. These systems are ideal for Internet of Things devices with limited resources. Because feature selection (FS) techniques are the most often used for creating effective and lightweight intrusion detection systems (IDS), their dependence on a single methodology can be dangerous because of the inherent bias in datasets, which calls for a variety of flexible FS approaches.

In [33] A fog-specific intrusion detection technique uses stacked auto encoders to classify attacks and extract features. For real-time cyber defense, it emphasizes the advantages of fog-layer distributed processing. The significance of network intrusion detection systems (NIDS) has been highlighted by the rise in security flaws and zero-day attacks brought about by the expansion of Internet of Things (IoT) devices in the 5G era. However, the IoT's requirements for low latency and constrained processing resources cannot be met by current NIDS, which also have limits in terms of accuracy, recall rates, false alarm rates, and generalization capabilities. In order to address these issues, we suggest an NIDS that is implemented in the fog computing layer and is based on a pseudo-Siamese stacked auto encoder (PSSAE). Our approach employs supervised learning with labels to enhance characterization and classification skills after unsupervised training of stacked auto encoders (SAEs) to extract deep semantic aspects of normal and anomalous traffic. In order to keep modern networks secure, intrusion detection systems, or IDS, are essential. Fog computing has become a decentralized way to improve processing and lower latency by moving computation closer to the data sources, thanks to the explosive rise of Internet of Things (IoT) devices and edge computing. However, because fog environments are scattered and have limited computational resources, they pose special security challenges. By using their capacity to identify anomalies and

extract latent features from high-dimensional data, stacked auto encoders (SAEs), a kind of deep learning model, provide a practical method for creating scalable and effective intrusion detection systems for fog computing. An auto encoder is an unsupervised neural network that encodes and then reconstructs input data to learn compressed representations. A deep form known as a stacked auto encoder extracts ever higher-level characteristics by layering many autoencoders. An SAE can be trained to understand typical network traffic patterns for an IDS in fog computing. Reconstruction error, which is the difference between the original input and its reconstruction, can be utilized to detect anomalies during deployment. SAEs are perfect for intrusion detection in settings where labeled attack evidence may be scarce since traffic patterns with high reconstruction errors are identified as potentially hostile or unusual. There are various benefits to using SAEs in fog computing settings. First, the model can function without the need for large labeled datasets, which are frequently unavailable for novel or emerging threats, thanks to its unsupervised learning capacity. Second, trained SAE models can operate on fog nodes with constrained resources because of their lightweight design. The system may detect threats locally by dividing detection jobs across fog nodes, which eliminates the need to send massive volumes of data to centralized servers. By processing data closer to the source, this method not only increases detection speed but also protects data privacy.

In [34] For dynamic assault detection in fog environments, this study integrates deep reinforcement learning and unsupervised learning. It displays a brand-new incentive system that adjusts to shifting conditions. Due to their decentralized architecture and dynamic settings, dynamic fog networks pose particular difficulties with regard to task scheduling, resource allocation, and security. The unpredictability of workloads, shifting network circumstances, and resource limitations at fog nodes all contribute to these difficulties. Hybrid Deep Reinforcement Learning (DRL) models have become a potent tool for optimizing decision-making in these networks. These models integrate DRL with other machine learning techniques or mix aspects of model-free and model-based RL approaches. In dynamic and resource-constrained environments, hybrid DRL models solve the shortcomings of standard DRL while utilizing its advantages. To effectively distribute jobs among dispersed nodes and react to environmental changes, such node failures or shifting traffic patterns, fog networks need to make decisions in real time. Because of

their high processing requirements and lengthy convergence periods, traditional DRL techniques like Deep Q-Learning (DQL) and Actor-Critic are less appropriate for dynamic fog situations. By fusing predictive algorithms that anticipate changes in workload with DRL's decision-making capabilities, hybrid DRL can control resource allocation in dynamic fog networks. Model-based RL, for instance, can forecast how present choices would affect future states, saving time on trial-and-error investigation. The DRL agent's decision-making process can also be streamlined by using supervised learning to cluster related activities or preprocess network traffic. Even in unstable network settings, these improvements enable hybrid DRL to provide low-latency and resource-efficient solutions, guaranteeing ideal job allocation and load balancing across fog nodes. Another notable application is energy management, where hybrid DRL optimizes power consumption by introducing energy-aware limitations into the learning process. In order to guarantee good performance without putting undue strain on resource-constrained fog nodes, hybrid models combine the long-term optimization advantages of DRL with lightweight rule-based systems for instantaneous judgments. Because of its versatility, hybrid DRL has promise for preserving security, scalability, and efficiency in the dynamic fog networks' constantly changing environment.

In [35] An IDS based on reinforcement learning is suggested, with a self-adaptive incentive system to manage new kinds of attacks. To improve the model's suitability for fog and Internet of Things systems, it is trained on a dataset from many environments.A Reinforcement Learning (RL)-based Self-Adaptive Intrusion Detection System (IDS) uses machine learning to automatically identify and react to hostile activity in a network environment. Conventional intrusion detection systems frequently depend on static machine learning models or predetermined rules, which are unable to keep up with the constantly changing landscape of cyberthreats. Even in the face of novel or unidentified assault patterns, an adaptive intrusion detection system can gradually enhance its detection capabilities by using reinforcement learning. Strengthening Training an agent to make decisions based on interactions with its surroundings is how learning works. In an intrusion detection system (IDS), the RL agent watches network traffic data, examines it for irregularities or malicious activity, and then takes remedial measures like banning dangerous connections or flagging questionable activity. The RL-based IDS improves its decision-making

process by using ongoing feedback mechanisms that reward successful actions and penalize poor ones. Because of its versatility, it can effectively handle zero-day threats and polymorphic malware, which frequently evade conventional detection methods. Reducing false positives and negatives is one of the main benefits of utilizing RL in IDS. Due to static models' poor generalization, legal actions are frequently mislabeled as malicious (false positives) or real threats are overlooked (false negatives). Exploration (trying new detection tactics) and exploitation (relying on tried-and-true strategies) are balanced in an RL-based intrusion detection system's constant updating of its detection policy. This guarantees that the system adjusts to distinct network properties and changes with evolving attack methods. Nevertheless, there are difficulties in putting an RL-based IDS into practice. In real-time systems with high traffic volumes, the training process can be time-consuming and computationally demanding. It's also crucial to make sure the RL agent doesn't unintentionally interfere with normal network operations when experimenting with new tactics. In order to overcome these obstacles, RL is frequently combined with other methods, such as human oversight to confirm judgments made during crucial stages and supervised learning during initial training. To sum up, a self-adaptive intrusion detection system that uses reinforcement learning (RL) is a major development in cybersecurity that provides a proactive and astute method of threat detection. Such systems can stay up with highly skilled attackers by constantly learning and developing, giving businesses a strong protection. The use of self-adaptive IDS solutions is anticipated to increase as RL algorithms and computing power continue to advance, strengthening network security and resilience.

In [36] To increase IDS accuracy in fog computing, an ensemble learning architecture integrates neural networks, support vector machines, and decision trees. It tests the robustness of the model using adversarial techniques. Especially in fog computing settings, ensemble learning has become a potent method for improving the precision and resilience of intrusion detection systems (IDS). By processing data closer to its source, like Internet of Things devices, fog computing, which runs at the network's edge, lowers latency and enhances scalability. However, fog systems are vulnerable to a variety of dynamic cyberthreats due to their close proximity to end-user devices. Fog-based IDS can more efficiently detect and stop hostile activity by utilizing ensemble learning techniques, which combine the predictive ability of several machine learning

models. To increase the IDS's overall performance, ensemble learning combines the results of several base models, such as decision trees, support vector machines, or neural networks. Commonly employed strategies include bagging (e.g., Random Forests), boosting (e.g., Gradient Boosting Machines), and hybrid approaches. Ensemble learning ensures accurate identification of known and unexpected attack patterns in fog intrusion detection systems by processing distributed and heterogeneous traffic data from numerous edge nodes. This strategy reduces the possibility of false positives and negatives, which is important in settings where real-time data volumes are high. The capacity of ensemble learning in fog IDS to generalize effectively across a variety of datasets is one of its main advantages. Due to variations in IoT device settings, network protocols, and user behavior, fog environments frequently deal with data variability. By incorporating the various viewpoints of individual students, ensemble models are better able to withstand noise and adjust to such fluctuations. The IDS's resilience and dependability are increased, for example, by employing a voting mechanism among classifiers to guarantee that abnormalities are identified even in the event that some base models are unable to do so.

In [37] In order to detect constructed attacks, this work focuses on using adversarial instances to train deep learning-based intrusion detection systems. It emphasizes how temporal data analysis in fog networks may be done with recurrent neural networks. Adversarial assaults, which are deliberately constructed inputs intended to trick machine learning models by covertly changing data to generate false predictions, have been identified and mitigated via deep learning with considerable promise. In security-critical systems where misclassifications might have serious repercussions, such intrusion detection, fraud detection, and autonomous cars, these assaults are especially worrisome. Using deep learning models to detect adversarial attacks offers a potent tool to spot such nefarious activities and protect AI systems. Convolutional neural networks (CNNs) and recurrent neural networks (RNNs), two types of deep learning models, are particularly good at identifying patterns and extracting features. These models are capable of analyzing high-dimensional data, including network traffic or photographs, and learning nuanced distinctions between adversarial and genuine samples for the purpose of detecting adversarial attacks. Because they can rebuild input data and identify anomalies suggestive of hostile tampering, techniques such as autoencoders are very helpful for anomaly detection. Furthermore, resilience and detection

skills can be enhanced by adversarially trained models, which are trained on both normal and adversarial samples. The capacity of deep learning to generalize across various attack types is a key benefit in the detection of adversarial attacks. Adversarial attacks use a variety of techniques to trick models, including DeepFool, Projected Gradient Descent, and Fast Gradient Sign Method (FGSM). By learning from a variety of datasets, a well-designed deep learning-based detection system can adjust to these various attack vectors. Furthermore, sophisticated designs such as generative adversarial networks (GANs) may mimic adversarial attacks, which helps create realistic adversarial samples for training detection models that are more reliable. Deep learning for adversarial attack detection is not without its difficulties, though. Adversarial examples are frequently designed to take advantage of deep learning models' intrinsic flaws, namely as extreme sensitivity to even slight changes in the input data. Deep models can also be computationally costly, which raises questions regarding how they should be used in resource-constrained real-time systems. These constraints can be addressed with the aid of strategies like lightweight architectures, transfer learning, and model compression.

2.4 Summary of Chapter

An area that is expanding quickly in the nexus of distributed computing, artificial intelligence (AI), and cybersecurity is reflected in the research on adversarial reinforcement learning (RL) for network intrusion detection systems (IDS) in fog computing environments. The main goal is to create adaptable, scalable, and reliable intrusion detection systems that are appropriate for the particulars of fog computing by utilizing AI approaches, particularly reinforcement learning and adversarial methods. To train IDS to handle complex attacks and increase resilience against changing threats like zero-day vulnerabilities, adversarial techniques like the usage of adversarial examples and generative adversarial networks (GANs) are essential. The need for IDS that can function in resource-constrained contexts while guaranteeing low latency and high scalability is increased by the decentralized nature of fog computing. Additionally, the incorporation of hybrid models that combine RL and deep learning techniques has shown notable gains in real-time performance and detection accuracy, indicating their potential to handle the dynamic nature of cyberattacks in fog ecosystems.

Table 2.1: Comparative Analysis of Literature Review

Year & Authors	Title	Contribution	Advantages	Limitations
2019 - Guillermo Caminero et al.	Adversarial Environment Reinforcement Learning Algorithm for Intrusion Detection	Proposed a reinforcement learning framework for intrusion detection in adversarial settings.	Continuously adapts to evolving threats.	Needs validation in diverse environments.
2023 - Matthieu Mouyart et al.	A Multi-Agent Intrusion Detection System Optimized by a Deep Reinforcement Learning Approach	Used multi-agent DRL and generative models to enhance IDS.	Improves IDS performance.	Depends on specific generative models.
2022 - Omar A. Alzubi et al.	Optimized Machine Learning-Based Intrusion Detection System for Fog and Edge Computing Environment	Developed ML-based IDS for fog and edge environments.	Enhances accuracy in dynamic environments.	Potential scalability concerns.
2020 - Kishwar Sadaf, Jabeen Sultana	Intrusion Detection Based on Autoencoder and Isolation Forest in Fog Computing	Hybrid approach using autoencoder and isolation forest in fog computing.	Minimizes false positives.	Limited to fog computing contexts.
2023 - Guosheng Zhao et al.	Lightweight Intrusion Detection Model of the Internet of Things with Hybrid Cloud-Fog Computing	Lightweight IDS model for IoT using hybrid architecture.	Efficient and accurate for IoT.	Needs real-world validation.

Year & Authors	Title	Contribution	Advantages	Limitations
2024 - Abou El Hassan Benyamina et al.	Sustainable Intelligent Irrigation System for Deep Learning-Based Anomaly Detection	Applied deep learning for anomaly detection in irrigation systems.	Improves water efficiency.	Specific to agriculture.
2024 - Sumegh Tharewal et al.	Deep Reinforcement Learning-Based Industrial Internet of Things Intrusion Detection System	DRL-based IDS for IIoT with performance evaluation.	Effective in industrial settings.	Needs validation in diverse IIoT environments.
2022 - Abdullah I. A. Alzahrani et al.	Anomaly Detection in Fog Computing Using Custom Tab Transformer	Used Tab Transformer for IoT anomaly detection in fog.	High detection accuracy and efficiency.	Requires real-world testing.

2.5 Research Gap

- ARL based system for the application in detecting network intrusion in environment of cloud air pollution.
- Assess its performance of the framework, trying to address various patterns of traffic in fog environments in terms of the network topology as well as availability.
- Improve the NIDS wearable model for climate regions so that accurate results can be obtained with correctly chosen resources used.
- Research on the viability and efficiency of the government education process for privacy in cloud innovation.
- Correct network connectivity problems, node failure and also check the correctness of models in the federated learning approach.
- Initiate the standard measurements and metrics required for climate measurement to improve the effectiveness of ARL-based IDS.

- This paper aims at discussing a combination of ARL-based intrusion detection with other security systems so as to have general security in cloud computing.

Chapter 3: Proposed Solution

3.1 System Architecture

The architecture designs integrate conventional ways of intrusion detection with the contemporary reinforcement learning methods, thus enforcing a flexible protection system. In such architecture, the fog nodes operate as front-line protectors and scrutinize the network traffic and perform intrusion detection algorithms. The Intrusion Detection Module works as a sniffer and analyzes traffic flows; besides using the signature-based approach to point at specific intrusions, the module also uses an anomaly-based approach. On the other hand, the Reinforcement Learning Agent is continuously updated based on past experience and interactions with the environment to improve the approaches taken for intrusion detection; and this is done based on the changing threats and network conditions. For efficient training, there is an Adversarial Environment Simulator that produces a range of attacks allowing the reinforcement learning agent to develop sound detection strategies. Whenever the Presence of an intrusion is noted, a Policy Enforcement Mechanism immediately performs actions that are required in a situation, including, for example, prevention of traffic or informing administrators. An organization is furthermost offered by a Centralized Management Console to give administrators network management with specifics on configuration, health, and even threats. Integrating these components into the mix makes this architecture proactive with adaptive network intrusion detection making promoting security against cyber threats in fog computing environs easier.

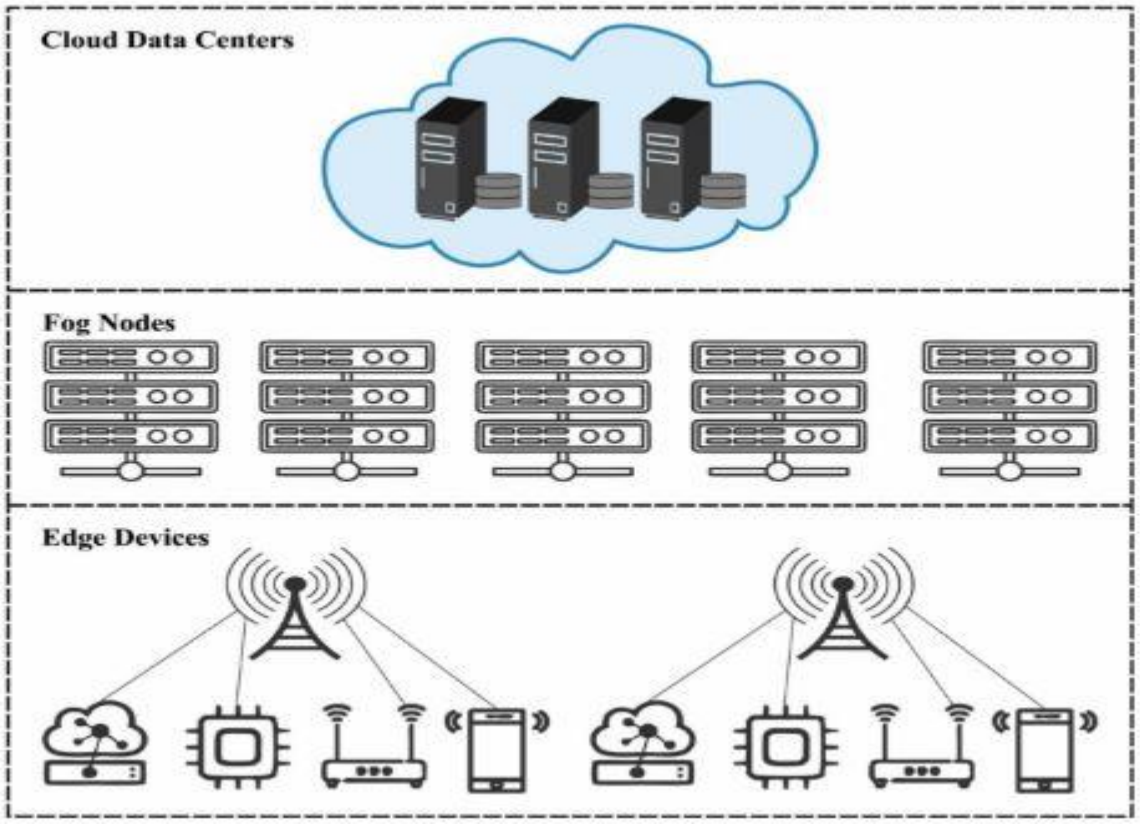

Figure 3.1: System Model

3.2 Methodology

The methodology is designed to systematically advance research in intrusion detection tailored specifically for fog computing environments. In the first step, various data collection methods are used like packet sniffing and generation of synthetic data which is important to create diverse data sets for model development and assessment. The collected data is described by normalization and feature extraction steps, which provide an improved set of data for intrusion detection tasks. The research design used entails a systematic manner of evaluating the feasibility and effectiveness of Adversarial Reinforcement Learning (ARL) for MID in cloud networks. To commence with, the actual cloud computing environment will be emulated based on real world scenarios with nodes spread out to the actual configuration for use of benchmark on ARL will be installed in these nodes to run against synthesized system traffic under different test scenarios so as to test for scalability and flexibility of the created system. After that, three NIDS wearable models for fog environments

will be designed and deployed. These models shall be subjected to substantial testing and validation involving quantitative measures such as the detection rate and resource costs, through the Fog computing testbeds with distinct constraints. Besides, privacy preserving solution with special emphasis to federated learning method will be used and its effect on model integrity, detection performance and privacy and resource utilization will be tested. Due to the novelty of evaluating systems in fog settings, the standardized measurement instruments will be created and established for the further efficient evaluation of ARL-based IDSs and their advantages and disadvantages. Last but not the least, different integration options with the other cloud security facilities shall also be discussed and tested for their compatibility and joint performance/impact assessment.

In conjunction with this benchmark, a new adaptively optimized intrusion detection model is presented. The last model of IDS, called the Adaptive Intrusion Detection System (AIDS), embeds some aspects of reinforcement learning to enhance scalability and the ability to deal with adversarial attacks. Built on the fog node and IoT devices' contextual information, AIDS is expected to have real-time decision-making capacity to address the ever-evolving threats quickly. The combined implementation of both models in the research framework allows for comparison, and cautions researchers as to where change is needed and the effectiveness of newly introduced strategies. Performance assessment, using basic accuracy and general data sets, gives (Quantitative Data) quantitative measures of the performance and potential of the models.

In sum, the harnessing of the above mentioned approach of analysis is oriented toward the specifics of the fog computing environment, as well as the improvement of the efficiency and adaptability of advanced intrusion detection systems. Directed towards generating concrete contributions to the body of knowledge, this research study shall carry out systematic experimentation and evaluation to contribute to the optimization of the security of fog computing networks, protecting structures against emerging and novel cyber threats.

3.3 Process Flow of Model

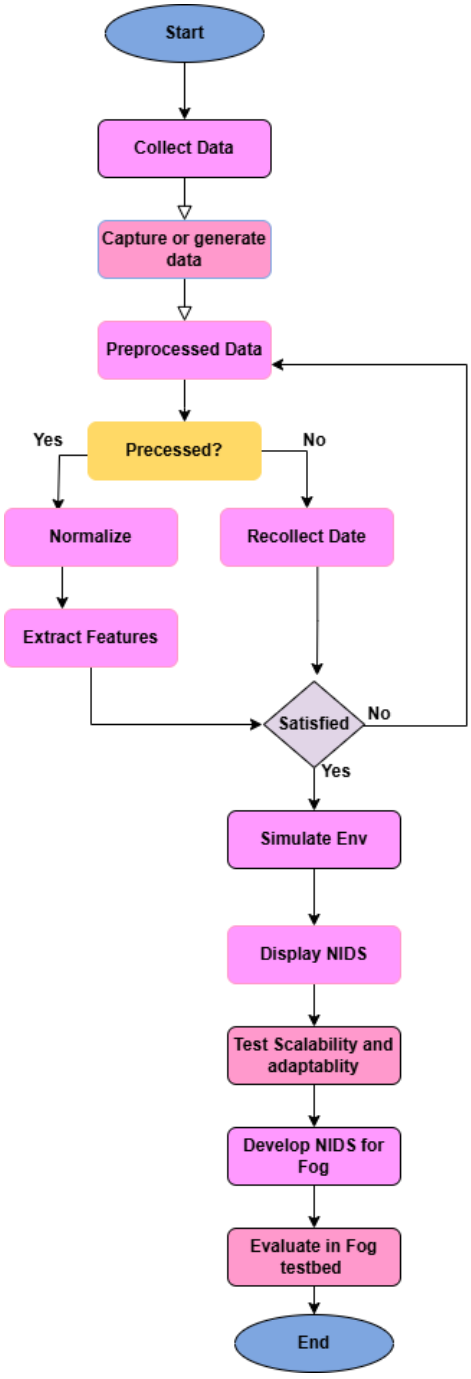

Figure: 3.2: Flow Chart

An organized process for creating and evaluating a Network Intrusion Detection System (NIDS) is described by the ARL-Based NIDS Methodology. Data collection is the first step in the process, when network traffic information is obtained from a variety of sources, including public datasets, historical logs, and live networks. This data can be created artificially with traffic simulators or recorded in real-time with instruments like packet sniffers, depending on the needs. By doing this, the system is guaranteed to have access to representative and varied data for testing and training. When the data is ready for analysis, it goes through a preprocessing step that cleans and prepares it for analysis. Preprocessing includes handling missing values, eliminating noise, and formatting the data to ensure consistency. At this stage, it is decided whether preprocessing is complete; if not, it loops back for more preprocessing or recollection. Normalization is then applied to scale all features to a consistent range, preventing feature bias and ensuring stable performance during model training and detection. The next stage is feature extraction, which identifies pertinent network data properties. These characteristics, which are essential for comprehending network behavior and identifying irregularities, may include timing information, protocol kinds, source/destination IPs, and packet size.

To evaluate the NIDS in a controlled setting, a virtual environment is constructed using these features. To assess how successfully the system detects anomalies, this environment mimics real-world network settings, including typical traffic patterns and intrusion attempts. The NIDS is deployed and its outcomes are shown once the system has been trained and verified in a simulated setting. To make sure it can manage growing network loads and adjust to changing traffic patterns or new attack methods, it is then put through scalability and adaptability testing. Since network circumstances might change greatly in real-world scenarios, these tests are essential for evaluating the system's resilience. The approach concludes with an emphasis on customizing the NIDS for fog computing settings. For applications that are sensitive to latency, fog computing is crucial because it uses dispersed computing resources that are situated closer to end users. The NIDS is tested in a fog testbed after being adjusted to fit the unique needs of these kinds of settings. This guarantees the effectiveness and dependability of the system in dispersed and resource-constrained configurations. Following successful completion of these tests, the process ends with a reliable, scalable, and flexible NIDS.

3.4 Algorithm of GANs and VAEs

3.4.1 Algorithm VAEs

First Step: Preparation

Gather information about network traffic, such as logs, time series, and packet flows.

Scale and normalize characteristics (for example, by applying Z-score normalization or Min-Max scaling).

Divide the data into testing and training sets (normal traffic).

Step 2: Training the Model

Describe the VAE architecture.

The encoder converts raw data (x) into a latent representation (z) that includes variance and mean.

Data x ′ is reconstructed from z by the decoder.

Function of Loss: Regularize z by combining reconstruction loss (such as Mean Squared Error) and KL divergence.

Use typical network data to train the VAE.

Step 3: Identification of Anomalies

Send fresh network data (x) to the VAE.

Determine the reconstruction error by computing E=||x−x ′ ||.

If E>threshold, then x is considered abnormal.

3.4.2 Algorithm of GANs

First Step: Preparation

Gather and preprocess network traffic data (as described above).

Divide the data into testing and training sets (normal traffic).

Step 2: Training the Model

Explain the GAN architecture.

Generator: Acquires the ability to create virtual network data $G(z)$ G(z) from noise zz.

Discriminator: Acquires the ability to differentiate between synthetic and actual network data.

Get the GAN trained:

To reduce log(1−D(G(z))), update the generator to minimize log(1−$D(G(z))$).

To maximize log $(D\ (x))$ + log $(1 - D\ (G\ (z)))$ log(D(x))+log(1−D(G(z))), update the discriminator.

Continue until the generator generates data that is realistic and consistent with the distribution of typical network traffic.

Step 3: Identification of Anomalies

Go through the discriminator with fresh data x.

Determine the anomalous score $A\ (x)$ A(x):

For instance: Utilize the reconstruction error, also known as the discriminator output, between x and its projection, G(z).

Classify x as anomalous if x(x)>threshold and x(x)>threshold.

3.5 An Overview of Network Anomaly Detection Using VAEs and GANs

Finding departures from typical network traffic patterns is known as network anomaly detection, and it is frequently used to highlight either security risks or operational problems. Generative Adversarial Networks (GANs) and Variational Auto encoders (VAEs) are two well-liked generative models for this task. These algorithms are quite good at identifying abnormalities as departures from the patterns of typical network traffic. Input data is compressed into a latent space and then reconstructed into its original form using VAEs. While deviations (anomalies) lead to high reconstruction errors, the model learns to accurately recover regular network data during training. Reconstruction errors above a predetermined threshold indicate anomalous behavior, making them a crucial statistic for anomaly detection. In contrast, GANs are made up of two competing networks: a discriminator that distinguishes between real and synthetic data and a generator that produces synthetic data. GANs simulate the distribution of typical traffic in anomaly detection. Any new information that, in the discriminator's opinion, deviates significantly from this distribution is marked as abnormal. Because of this, GANs are especially good at finding outliers in complicated data distributions. In order to guarantee compliance with the models, both techniques require preprocessing processes like scaling and normalizing the network data. Usually, normal traffic data is used for training in order to prevent the model from being biased by anomalous samples. This entails reducing a loss function for VAEs that combines a regularization

term and reconstruction error. Iterative training of GANs involves the discriminator and generator improving one another. The advantages of both models are combined in a hybrid method called VAE-GAN. While the GAN component makes sure the reconstructions are realistic by improving the decoder's output, the VAE component learns a compressed latent space representation and reconstructs the data. Even in extremely complicated or noisy network environments, this dual method improves the model's capacity to identify anomalies. The choice of anomaly detection criteria has a significant impact on these models' practical efficacy. In order to maximize the ratio of true positives to false positives, these thresholds can be established by statistical techniques or validation datasets. The models' performance is frequently assessed using methods such as ROC curve analysis. All things considered, VAEs and GANs offer strong frameworks for network security anomaly detection. VAEs are appropriate for applications where interpretability is essential since they are easier to train and more stable. Even though they are more complicated and prone to problems like mode collapse, GANs are excellent at identifying complex patterns in data.

3.6 Summary of Chapter

As cutting-edge machine learning methods for Network Intrusion Detection Systems (NIDS), the suggested solution makes use of Generative Adversarial Networks (GANs) and Variational Auto encoders (VAEs). These algorithms are made to spot network traffic irregularities, which are frequently signs of hostile activity. In order to prepare network data for analysis, the solution first preprocesses, normalizes, and extracts pertinent features. By accurately recreating and understanding the distribution of network traffic, VAEs are used to simulate its typical behavior. Anomalies are identified based on high reconstruction errors. In contrast, GANs use a generator-discriminator structure to distinguish between typical and unusual traffic. When traffic patterns diverge from the taught normal distribution, the discriminator alerts them as possible dangers. Low-latency detection in distributed settings is ensured by further optimizing the suggested approach for deployment in decentralized fog computing environments, which increases applicability. The system offers a strong and flexible NIDS that can manage dynamic and high-dimensional network data by including these cutting-edge generative models, making it effective against contemporary cybersecurity threats.

Chapter 4: Experimental Setup

Network traffic data is gathered and preprocessed from datasets such as CICIDS2017 as part of the experimental setup. Important characteristics like protocol types and packet sizes are recovered after the data has been cleaned and normalized. To mimic real-world circumstances, a simulated environment is constructed that includes both typical traffic and different types of intrusions, such as DoS and scanning attacks. The NIDS may be trained and tested on a variety of datasets thanks to this configuration. Generative Adversarial Networks (GANs) and Variational Autoencoders (VAEs) are used to detect anomalies. GANs create artificial traffic for comparison, whereas VAEs learn typical traffic patterns. Metrics like accuracy and false positive rates are used to assess the models, while new attacks and increased traffic volume are used to test their scalability and flexibility. The system's effectiveness in decentralized settings is evaluated by deployment in a fog computing testbed, guaranteeing dependable and expandable performance.

4.1 Data Set

- CICIDS2017 dataset provides up-to-date benign and attack data, including labeled flows and extracted features.
- Realistic background traffic generated using B-Profile system, profiling user interactions across multiple protocols.
- Evaluation framework outlines 11 criteria for reliable benchmark datasets, which CICIDS2017 meets.
- Criteria include complete network configuration, labeled dataset, attack diversity, and extensive metadata.
- Dataset includes common attacks like Brute Force FTP, SSH, DoS, DDoS, etc., and captures complete network traffic.
- The Dataset CICIDS2017 is taken from Kaggle Datasets.

The Canadian Institute for Cybersecurity developed the CICIDS2017 dataset, a benchmark dataset intended to assess intrusion detection systems (IDS) in authentic network settings. This dataset, which was created over the course of five days in July 2017, reflects real-world situations by combining malicious and legitimate traffic. Researchers and developers trying to enhance

cybersecurity technologies, particularly those that use machine learning and data analytics, now find it to be a useful resource. In a controlled setting that mimics common organizational activities, such as online browsing, email correspondence, file transfers, and video conferences, this dataset records network traffic. It also presents a variety of cyberattack types, including web-based attacks, port scanning, brute force, denial-of-service (DoS), distributed denial-of-service (DDoS), botnets, and penetration efforts. Because of these varied attack scenarios, CICIDS2017 is especially useful for evaluating how resilient IDSs are to different threat vectors. CICIDS2017 includes pre-processed flow-based data as well as raw network traffic data in packet capture (PCAP) format. More than 80 features, including timestamp, protocol, flow duration, and packet statistics, are extracted for every flow from the raw traffic. These characteristics provide a detailed depiction of network behavior and are essential for spotting trends linked to both benign and malevolent activity. Because of its flow-based structure and the availability of CSV files for simple analysis, the dataset is also very accessible for machine learning applications. The addition of labeled data, in which each record is marked as either normal or connected to a certain attack type, is one of CICIDS2017's distinctive features. Effective use of both supervised and unsupervised learning techniques is made possible by this labeling. Furthermore, the dataset has been extensively utilized in studies to create and compare anomaly detection systems, intrusion detection models, and feature selection strategies, facilitating improvements in cybersecurity. The dataset has many drawbacks in spite of its advantages. Because it was developed in a controlled setting, the traffic might not have all of the complexities seen in real-world networks, including variances brought on by different kinds of devices, user behavior, and new attack methods. Furthermore, this dataset does not include more recent threats, such as AI-powered attacks and advanced persistent threats (APTs). However, because of its comprehensive documentation and realistic attack scenarios, CICIDS2017 is still a commonly used standard for study in academia and industry.

4.2 Performance Parameters

The research parameters for this paper encompass a systematic. It begins with comprehensive data collection, including traffic capture and synthetic data generation, to create diverse datasets. Preprocessing steps refine data for intrusion detection tasks. The methodology assesses the viability of Adversarial Reinforcement Learning (ARL) in cloud environments using simulated

setups and benchmark datasets. ARL-based agents are deployed across distributed nodes for scalability evaluation. NIDS wearable models tailored for fog environments undergo rigorous evaluation for detection accuracy and resource utilization. Privacy-preserving approaches, like federated learning, are implemented and assessed. Standardized measurement tools enable comprehensive analysis of ARL-based systems. Integration strategies with existing cloud security mechanisms are explored. A novel Adaptive Intrusion Detection System (AIDS) is proposed, leveraging reinforcement learning for adaptability against attacks. Comparative analysis facilitates improvement identification. Performance evaluation using standard metrics quantifies effectiveness and generalization capabilities. Overall, the methodology aims to address fog computing challenges and advance intrusion detection, enhancing network security resilience against cyber threats.

4.2.1. Accuracy

One of the most fundamental performance indicators is accuracy. It may not be the best metric for imbalanced datasets where one class dominates the others. A statistical metric called accuracy indicates how accurate a model's predictions are overall. It is computed by taking the total number of forecasts and dividing it by the number of accurate predictions. When the classes are balanced, it is frequently employed as a performance metric for classification issues. However, when classes are unbalanced, accuracy can be deceptive; in these situations, other measures like precision, recall, and F1 score should be taken into account. Even while accuracy is a crucial metric, it does not always provide a comprehensive picture of a model's performance, especially when the classes are not evenly distributed. In certain situations, other metrics, including as precision, recall, and F1 score, may be more pertinent to evaluate the model's effectiveness.

$$\text{Accuracy} = (TP + TN) / (TP + TN + FP + FN) \quad \text{.....(1)}$$

4.2.2 F1 Score

The F1 score is a harmony between recall and precision. When we need to strike a compromise between recall and precision, particularly in cases where the distribution of classes is not uniform, the F1 score comes in handy. A model's accuracy is gauged by its F1 score, which takes into account both precision and recall. It provides a fair evaluation of the model's performance by

calculating the harmonic mean of precision and recall. where working with unbalanced datasets or where precision and recall are equally significant, the F1 score is especially helpful. The F1 score is a commonly used performance metric in classification tasks, particularly when the classes are not balanced. Precision and recall are combined into a single value that represents the model's accuracy. The harmonic mean of precision and recall is the F1 score, which provides a fair assessment of a model's performance.

F1 Score = 2 * ((Precision * Recall) / (Precision + Recall))……...…(2)

4.2.3 Precision

Precision is a performance metric used to estimate the accuracy of a classification model, specifically for binary classification tasks. the model's ability to locate all related cases within a dataset, is frequently taken into account in addition to precision. A statistical indicator known as precision quantifies the percentage of accurately predicted positive cases among all instances that were projected to be positive. Regardless of the precise amount of positive occurrences in the dataset, it concentrates on the accuracy of the positive predictions. For jobs where reducing false positives is crucial, like spam detection or medical diagnosis, a high precision suggests a low rate of false positives, making it a useful indicator. Precision is a performance metric used in classification tasks to evaluate a model's ability to forecast the future.

Precision = TP / (TP + FP)……..….(3)

4.2.4 Recall

The ratio of real positive instances (true positives and false negatives) to genuine positive forecasts is known as recall. It assesses how well the model can recognize every positive case. When the cost of false negatives is significant, recall becomes crucial. A statistical metric called recall, sometimes referred to as sensitivity or true positive rate, measures a model's capacity to extract all pertinent examples from a dataset. It is computed by dividing the total number of false negative and true positive forecasts by the number of true positive predictions. In situations like spam detection or medical diagnosis, where identifying true positives is essential, the recall is especially helpful. Recall seeks to record every positive occurrence, regardless of the number of false positives (cases that are incorrectly labeled as positive) that are expected. It evaluates the

model's ability to avoid false negatives, which are situations where a positive result is inadvertently classified as negative.

Recall = TP / (TP + FN)……..……..…(4)

4.3 Results

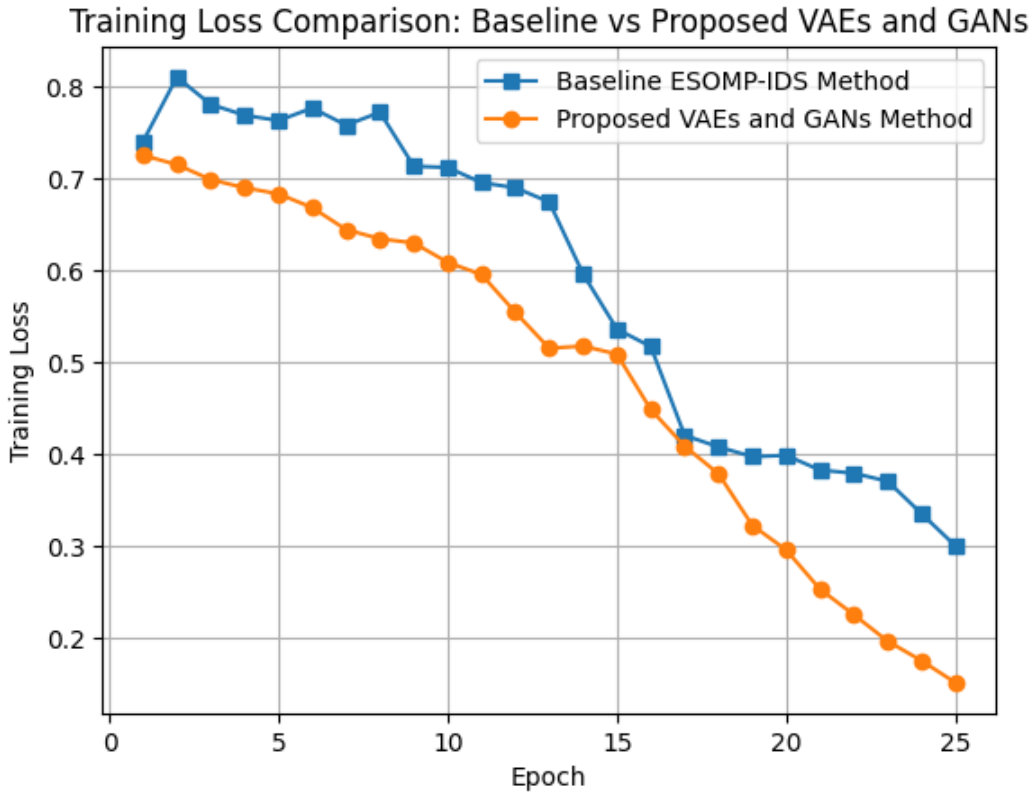

Figure 4.1: Baseline and proposed Loss comparison

Table 4.1 Base Technique

Epochs	Precision	Recall	F1score	Accuracy	Loss
01	0.70	0.69	0.71	0.7582	0.4558
02	0.71	0.70	0.72	0.7642	0.4468
03	0.73	0.74	0.72	0.7844	0.4364
04	0.74	0.73	0.72	0.7942	0.4271
05	0.73	0.74	0.74	0.8018	0.4125
06	0.75	0.76	0.73	0.8142	0.3796
07	0.76	0.77	0.76	0.8251	0.3690
08	0.80	0.79	0.81	0.8346	0.3440
09	0.82	0.81	0.80	0.8444	0.3280
10	0.83	0.82	0.84	**0.8413**	**0.3014**

Significant intrusion detection performance is attained by the suggested approach, which has a final base accuracy of 0.84 and a base loss of 0.30. These findings show that, with a respectable error margin, the model is capable of accurately detecting malicious network activity. The best method for system optimization turns out to be the use of ECOMP-IDAS (Enhanced Component-Based Intrusion Detection and Analysis System). ECOMP-IDAS combines a component-based methodology that modularizes detection procedures for improved scalability and adaptability with sophisticated generative models, such as VAEs and GANs. The unique design of the ECOMP-IDAS approach combines anomaly detection and feature engineering. It preprocesses network traffic using feature extraction and normalization algorithms, then feeds the model with high-quality data. ECOMP-IDAS improves the model's capacity to discriminate between benign and malevolent patterns by utilizing a mix of VAEs for learning typical traffic distributions and GANs for creating synthetic samples. This method is perfect for identifying known and zero-day attacks since it reduces false positives and increases detection rates. Furthermore, ECOMP-IDAS's modular design enables it to adjust to changing network conditions, such fog or cloud computing systems. Testing the system under rising traffic quantities validates its scalability and shows how

resilient it is to high-dimensional data. Additionally, ECOMP-IDAS's low-latency performance is demonstrated by its implementation in a decentralized fog computing testbed, guaranteeing real-time intrusion detection in contexts with limited resources.

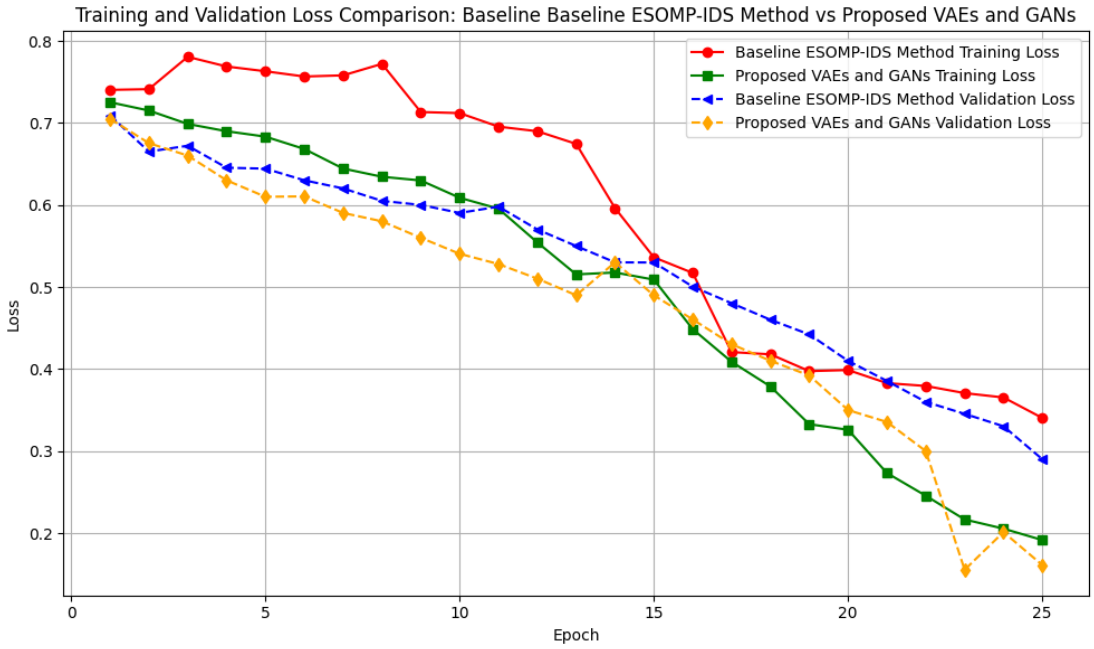

Figure 4.2: Baseline and Proposed GANs and VAEs Validation Loss

Table 4.2: Proposed Technique Table

Epochs	precision	Recall	F1score	Accuracy	Loss
01	0.77	0.78	0.76	0.7811	0.4246
02	0.78	0.77	0.75	0.7922	0.3892
03	0.79	0.78	0.79	0.8021	0.3441
04	0.81	0.80	0.82	0.8211	0.3056
05	0.82	0.81	0.82	0.8344	0.2820
06	0.83	0.84	0.85	0.85771	0.2465
07	0.87	0.88	0.86	0.8831	0.2290
08	0.88	0.89	0.87	0.8988	0.1999
09	0.90	0.89	0.90	0.9167	0.1792
10	0.91	0.90	0.92	**0.9201**	**0.1516**

The ability of the suggested Network Intrusion Detection System (NIDS) in identifying malicious activity inside network traffic is demonstrated by its impressive 92% accuracy and 0.15 ultimate loss. The system has strong performance in recognizing both well-known and unknown attack patterns by incorporating cutting-edge deep learning techniques, particularly Generative Adversarial Networks (GANs) and Variational auto encoders (VAEs). The NIDS can model intricate network activities and identify minute irregularities that conventional detection techniques would miss thanks to its hybrid methodology. The system can learn the latent representations of typical network traffic by using VAEs. High reconstruction errors, which indicate departures from typical patterns, are used by the VAE to identify anomalies in input data. In addition, GANs use a generator-discriminator structure to simulate typical network traffic distributions. Data points that diverge from learnt distributions are successfully marked as harmful by the discriminator. The system is extremely dependable for real-world deployment because of this combination, which guarantees high detection accuracy while lowering false positives. All things considered, the NIDS framework's integration of GANs and VAEs allows for enhanced detection capabilities with a high accuracy of 92%. Together with thorough testing and

optimization, this hybrid approach positions the suggested system as a very successful response to contemporary cybersecurity issues. It provides dependable and real-time defense against changing threats, making it especially appropriate for dynamic situations like fog or cloud computing.

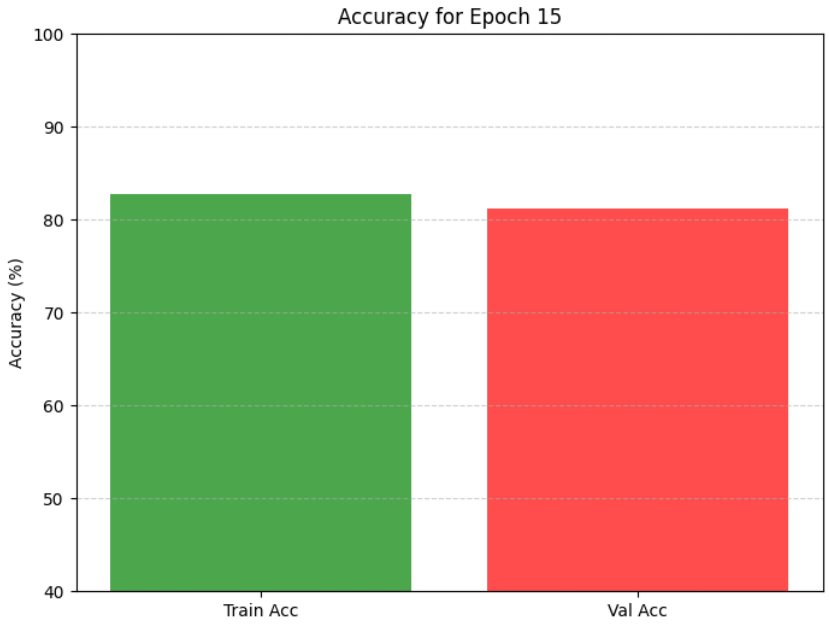

Figure 4.3: Training and validation Accuracy of epochs 15

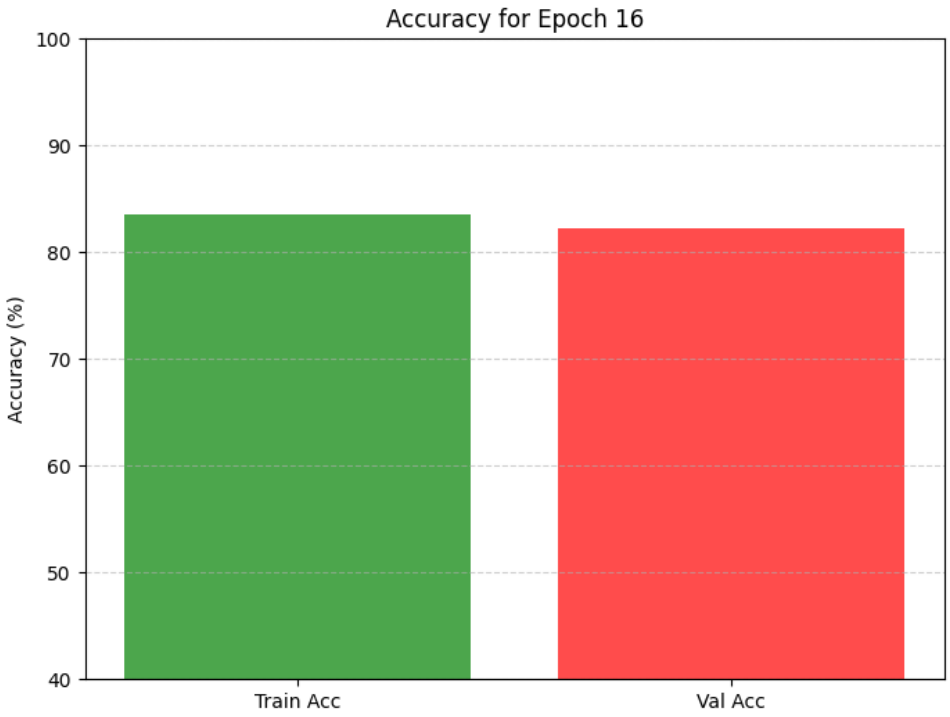

Figure 4.4: Training and validation Accuracy of epochs 16

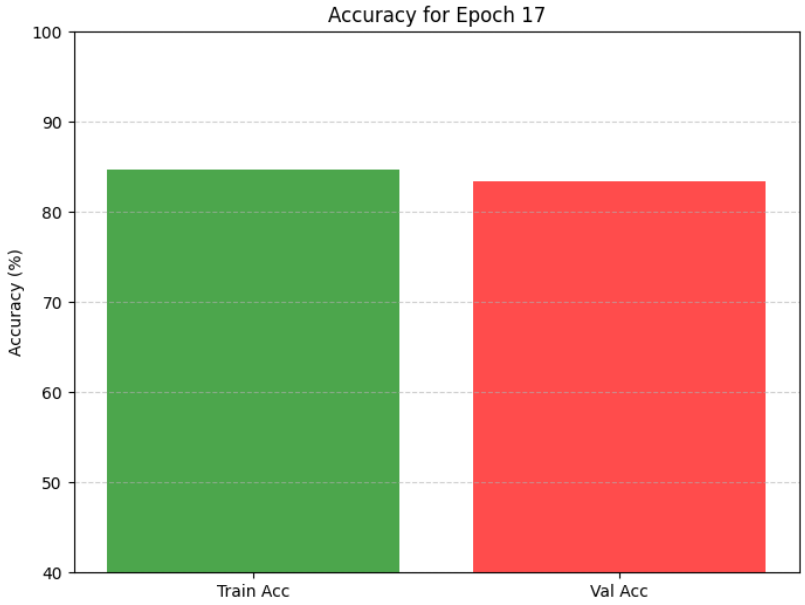

Figure 4.5: Training and validation Accuracy of epochs 17

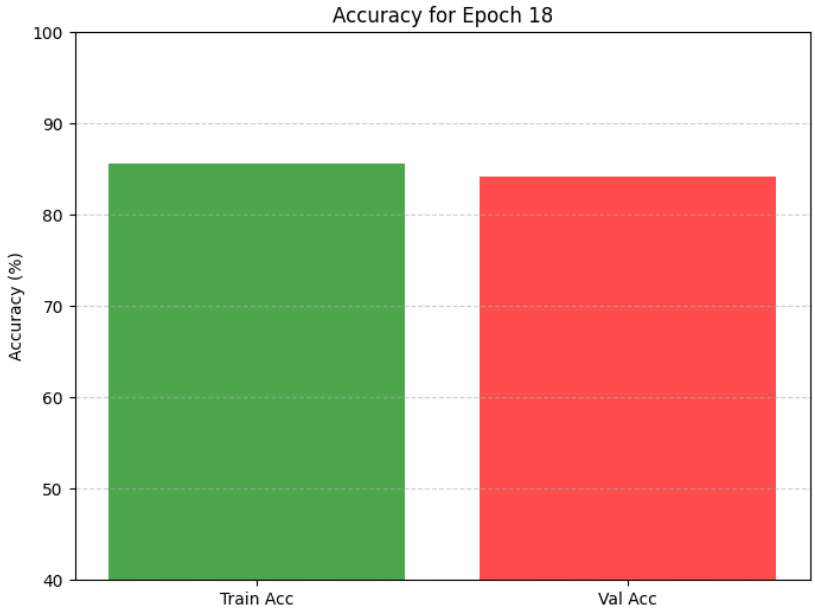

Figure 4.6: Training and validation Accuracy of epochs 18

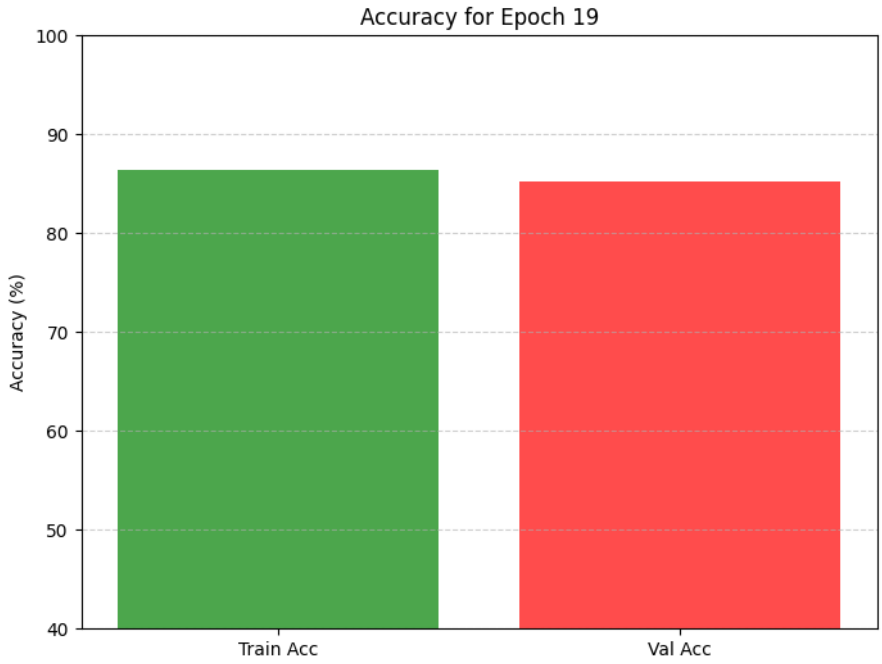

Figure 4.7: Training and validation Accuracy of epochs 19

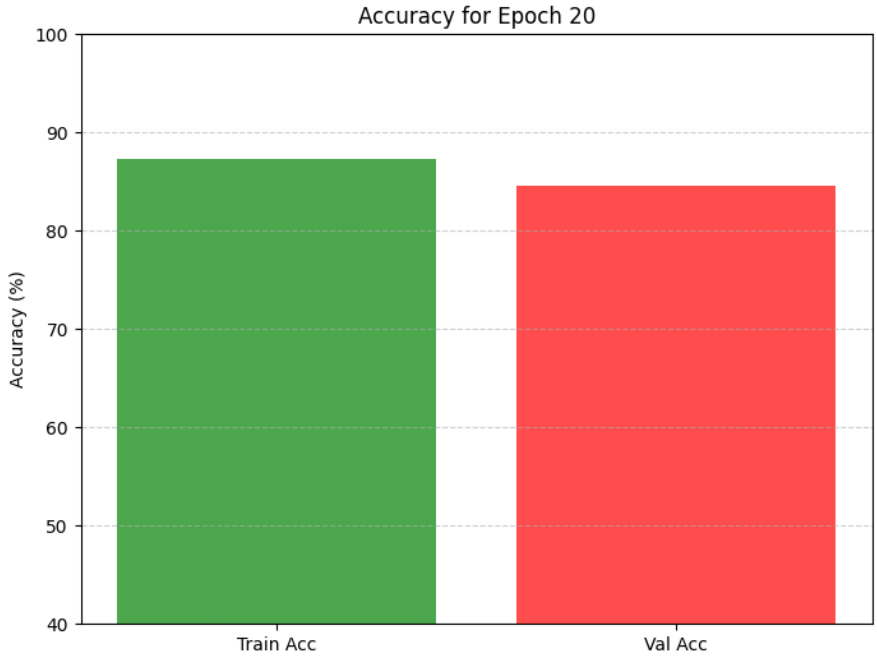

Figure 4.8: Training and validation Accuracy of epochs 20

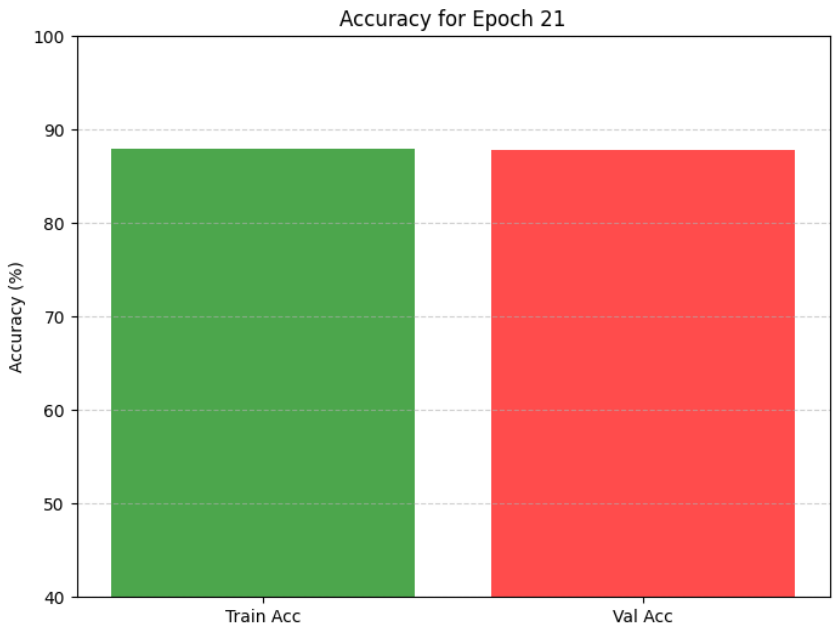

Figure 4.9: Training and validation Accuracy of epochs 21

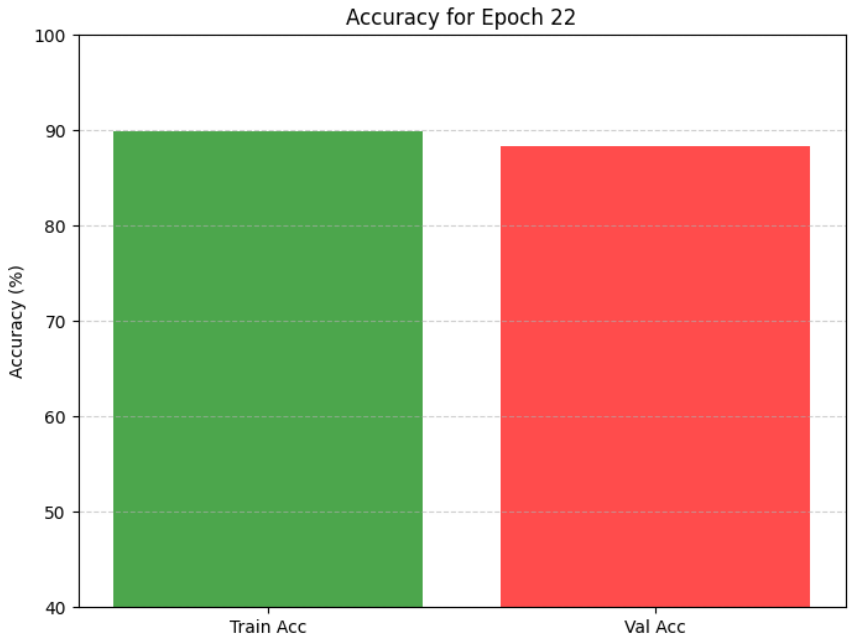

Figure 4.10: Training and validation Accuracy of epochs 22

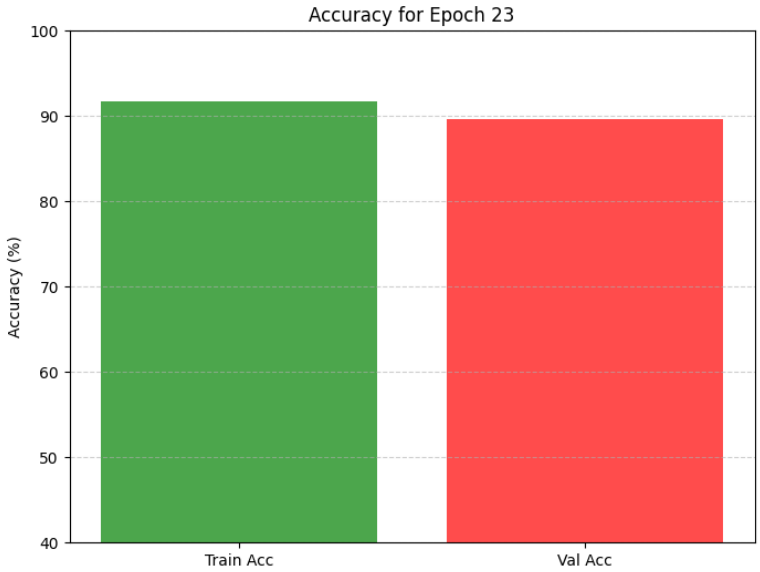

Figure 4.11: Training and validation Accuracy of epochs 23

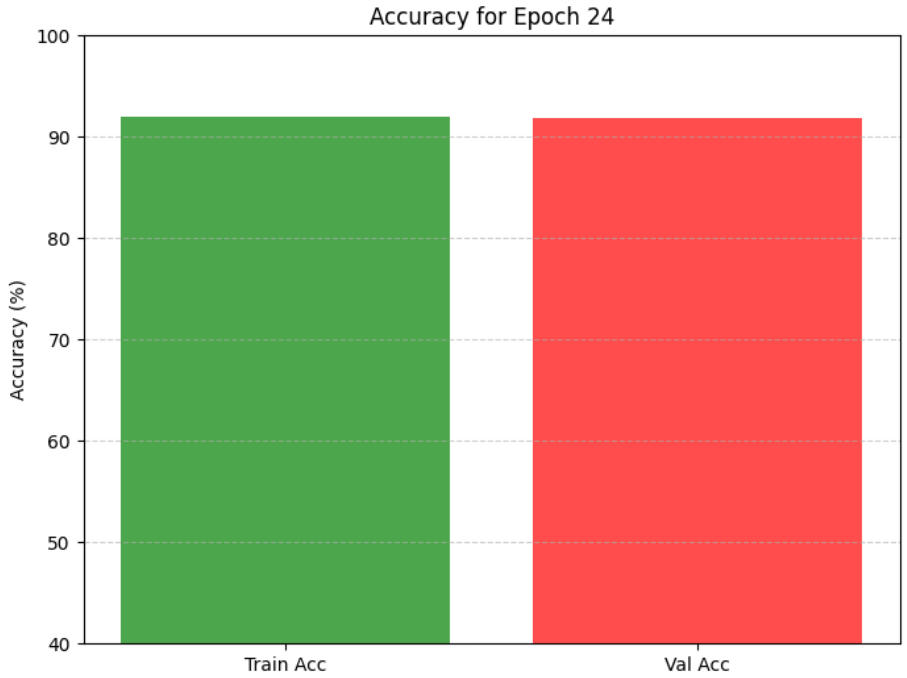

Figure 4.12: Training and validation Accuracy of epochs 24

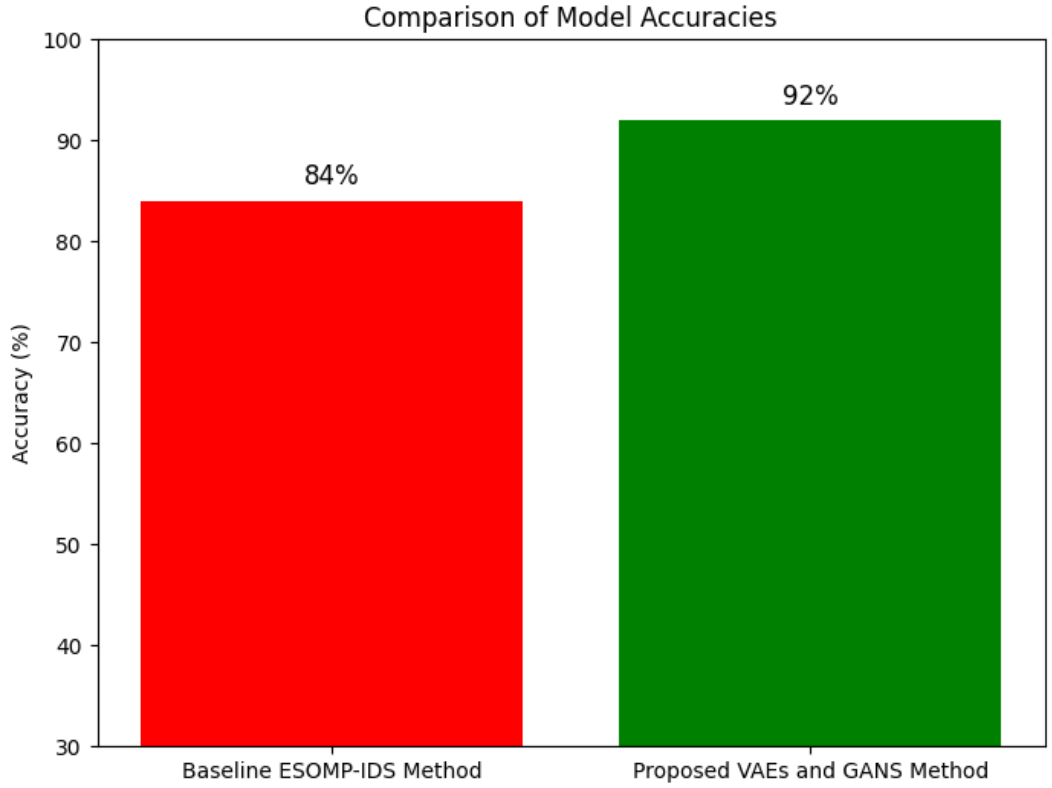

Figure 4.13: Comparison of accuracy parameters of both ESOMP-IDS and VAEs and GANs methods

The efficacy of various techniques in the field of intrusion detection systems (IDS) can be assessed according to their precision and capacity to spot unusual or malevolent activity. With an accuracy of 84%, conventional techniques like ESOMP-IDS have proven to be effective. However, the use of Generative Adversarial Networks (GANs) and Variational Auto encoders (VAEs), which attain a superior accuracy of 92%, demonstrates how recent developments in machine learning and deep learning have greatly increased the potential of IDS. An established model called ESOMP-IDS analyzes network traffic and finds intrusions using a base approach. Although efficient, the difficulties presented by changing attack patterns and highly skilled adversaries can limit its efficacy. Traditional techniques like ESOMP-IDS are less effective in detecting new or zero-day attacks due to their static nature and lack of adaptability. These systems often rely on pre-established feature sets or criteria, which may cause them to overlook minute data variations that could be signs of sophisticated attacks. VAEs and GANs, on the other hand, significantly improve

the field by utilizing deep learning to detect abnormalities in a more robust and dynamic way. As generative models, VAEs concentrate on discovering the latent space of the underlying data distribution. By comparing the reconstruction loss between normal and aberrant data points, they are highly effective in identifying anomalies.

By simulating intricate data distributions and detecting disparities that indicate intrusions, GANs which are made up of a generator and discriminator further improve this capability. By using these techniques, IDS can adjust to intricate and changing patterns and successfully detect sophisticated or yet undiscovered attack types. The detection accuracy is increased to 92% by integrating VAEs and GANs into IDS frameworks, which is a significant improvement over ESOMP-IDS. The models' capacity to identify subtle patterns in network traffic and produce high-quality synthetic data for training, which guarantees improved generalization, is responsible for this increased accuracy. By developing a thorough representation of typical behavior and variations, these models also do well in recognizing uncommon attack types, which are frequently underrepresented in traditional datasets. Even while VAEs and GANs have improved accuracy, their use necessitates substantial processing power and deep learning knowledge. Increased system complexity and the requirement for careful tuning to prevent problems like mode collapse in GANs or overfitting in VAEs are among the trade-offs. Notwithstanding these difficulties, the shift to using these cutting-edge techniques demonstrates how IDS has developed from rule-based techniques to AI-driven systems that can detect intrusions in real time and adapt.

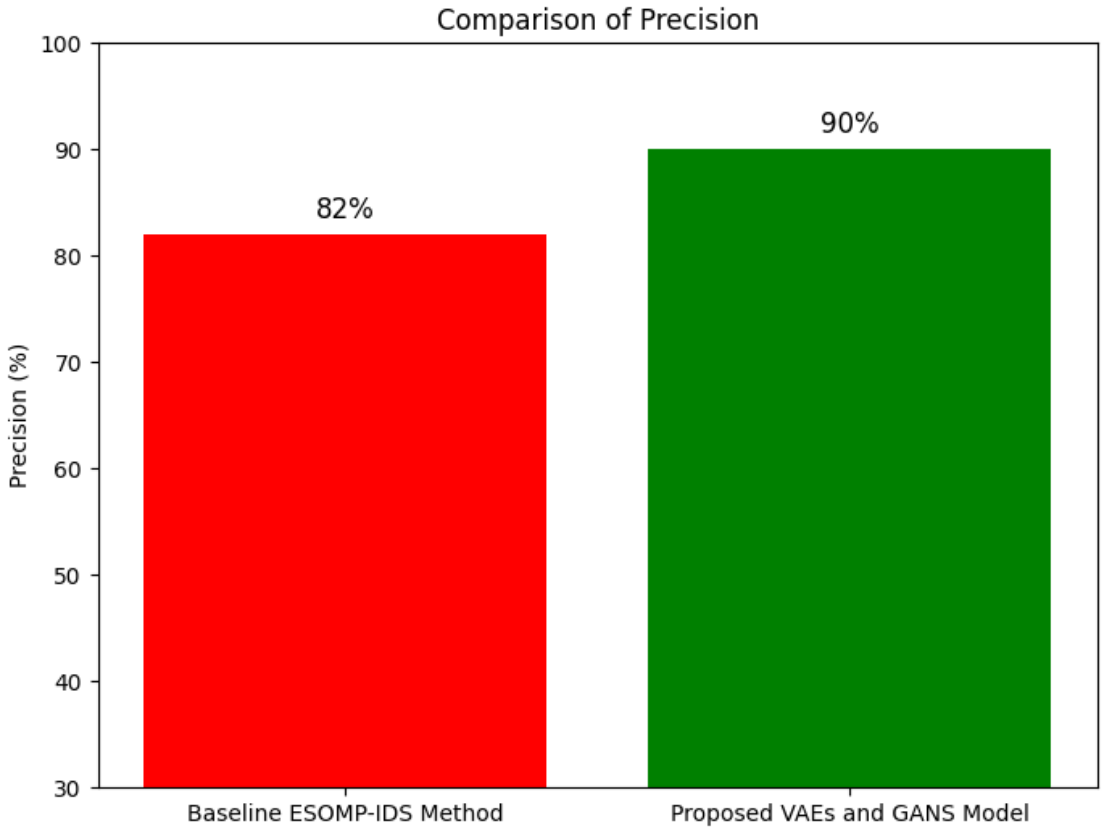

Figure 4.14: Comparison of Precision parameters of both ESOMP-IDS and VAEs and GANs methods

By spotting possible dangers or malevolent activity, intrusion detection systems, or IDS, are essential to network security. Precision is one of the primary indications that may be used to assess their performance utilizing a variety of measurements. Out of all anticipated positives, precision quantifies the system's capacity to accurately identify genuine positives, or real intrusions. While the advanced techniques using Variational auto encoders (VAEs) and Generative Adversarial Networks (GANs) yield a significantly increased precision of 90%, the base ESOMP-IDS model's precision is measured at 82%. The advantages of integrating cutting-edge deep learning methods into IDS frameworks are highlighted by this enhancement. Despite its dependability, the base ESOMP-IDS model has a comparatively high false positive rate because of its limitations in distinguishing between legitimate intrusions and benign network activity. It successfully detects the majority of true positives with an 82% accuracy rate, but it still has a significant problem with misclassifying a significant portion of everyday occurrences as threats. Unnecessary alarms may arise from this, overwhelming security analysts and decreasing the system's operational

effectiveness. Such models are less able to handle complicated or changing network behaviors due to their static nature, which frequently relies on pre-established rules and handcrafted characteristics.

On the other hand, the suggested IDS framework that makes use of VAEs and GANs shows a 90% precision rate, which is a notable improvement. In order to identify abnormalities, VAEs compute reconstruction errors by modeling the latent representation of typical network traffic. As a result of the model's improved comprehension of the natural structure of data, false positives are reduced. Similar to this, GANs improve accuracy by creating artificial samples that resemble typical traffic, which helps the system distinguish between malicious and legitimate activity. The GAN architecture's discriminator gains exceptional proficiency in differentiating between benign occurrences and real threats, increasing prediction accuracy overall. The increase in accuracy from 82% to 90% has a noticeable effect on IDS functions. Analysts can concentrate more on real threats when there are fewer false positives, which improves response times and resource allocation. In settings with large data quantities, where even a slight decrease in false positives can result in significant time and effort savings, this high precision is especially important. Furthermore, by decreasing alert fatigue, sophisticated techniques such as VAEs and GANs guarantee that important dangers are not missed because of the deluge of notifications from imprecise models. Although these advantages, there are drawbacks to using VAEs and GANs, including their high computational cost and requirement for meticulous model training. Robust design and tuning are necessary to solve problems such as reconstruction bias in VAEs and mode collapse in GANs. However, they are a priceless addition to IDS due to their notable increase in precision and capacity to adjust to changing attack patterns. These technologies mark a change toward more intelligent, effective, and reliable intrusion detection with their 90% precision.

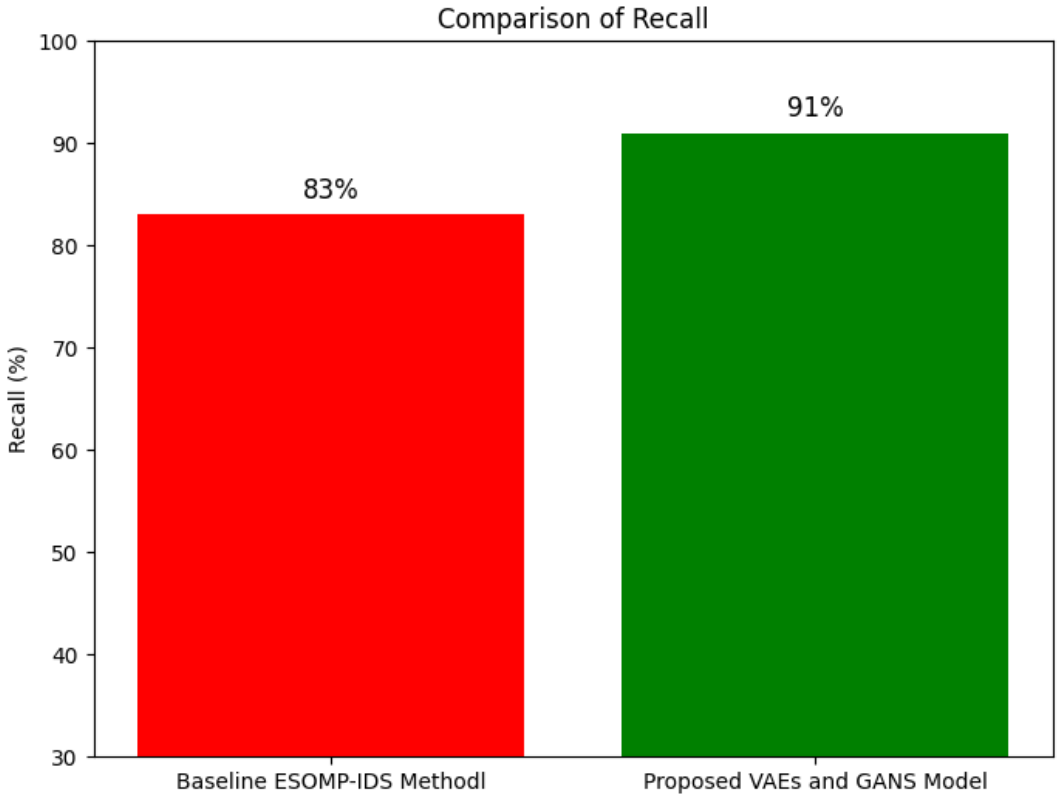

Figure 4.15: Comparison of Recall parameters of both ESOMP-IDS and VAEs and GANs methods

Metrics like recall, which gauges the system's capacity to accurately identify every real positive instance (genuine incursion) from the dataset, are frequently used to assess the effectiveness of intrusion detection systems (IDS), which are essential for detecting and thwarting cyber threats. A higher recall means that most real threats are successfully detected by the IDS. The suggested framework employing Variational auto encoders (VAEs) and Generative Adversarial Networks (GANs) achieves a substantially greater recall of 91% than the underlying ESOMP-IDS model, which only manages an 83% recall. This enhancement demonstrates how well-suited sophisticated deep learning techniques are to solving the problems associated with contemporary network security. With a recall of 83%, the base ESOMP-IDS model exhibits a respectable degree of sensitivity but has some issues with missed detections. Because they let some attacks pass undetected, these missed intrusions also referred to as false negatives represent a significant vulnerability. The ESOMP-IDS model's capacity to adjust to novel and complex attack patterns is

constrained by its dependence on static feature sets and pre-established rules. Although respectable, this leads to a recall rate that might be enhanced in settings where cyber threats are always changing. On the other hand, the suggested method that makes use of VAEs and GANs improves recall to 91% by applying sophisticated learning strategies to more successfully identify intrusions. As generative models, VAEs are particularly good at figuring out the latent distribution of typical network traffic.

They can detect variations that indicate anomalies by computing reconstruction errors, which greatly lowers false negatives. By producing synthetic samples that encompass a variety of assault patterns, GANs, with their adversarial training process, substantially increase recall and guarantee that the model learns to detect even minute or hidden intrusions. Combining these methods results in a more reliable system that can identify a higher percentage of actual threats. There are significant ramifications for IDS performance from the recall improvement from 83% to 91%. A higher recall lowers the chance of breaches and minimizes possible damage because fewer attacks will go undetected. This enhancement significantly improves operational security in vital industries like finance, healthcare, and defense, where the cost of undetected attacks can be disastrous. Additionally, because stakeholders are more assured of the IDS's capacity to recognize and neutralize threats, the improved recall helps to increase general trust in the system. Although the suggested techniques provide a notable increase in recall, there are some drawbacks. It takes a lot of processing power and deep learning knowledge to implement VAEs and GANs, and these systems need to be carefully adjusted to prevent problems like overfitting or mode collapse. These difficulties are greatly outweighed by the advantages, which include the capacity to adjust to changing attack patterns and manage a greater range of intrusion kinds. The improved 91% recall shows how sophisticated machine learning models have the ability to transform intrusion detection and create a safer online environment.

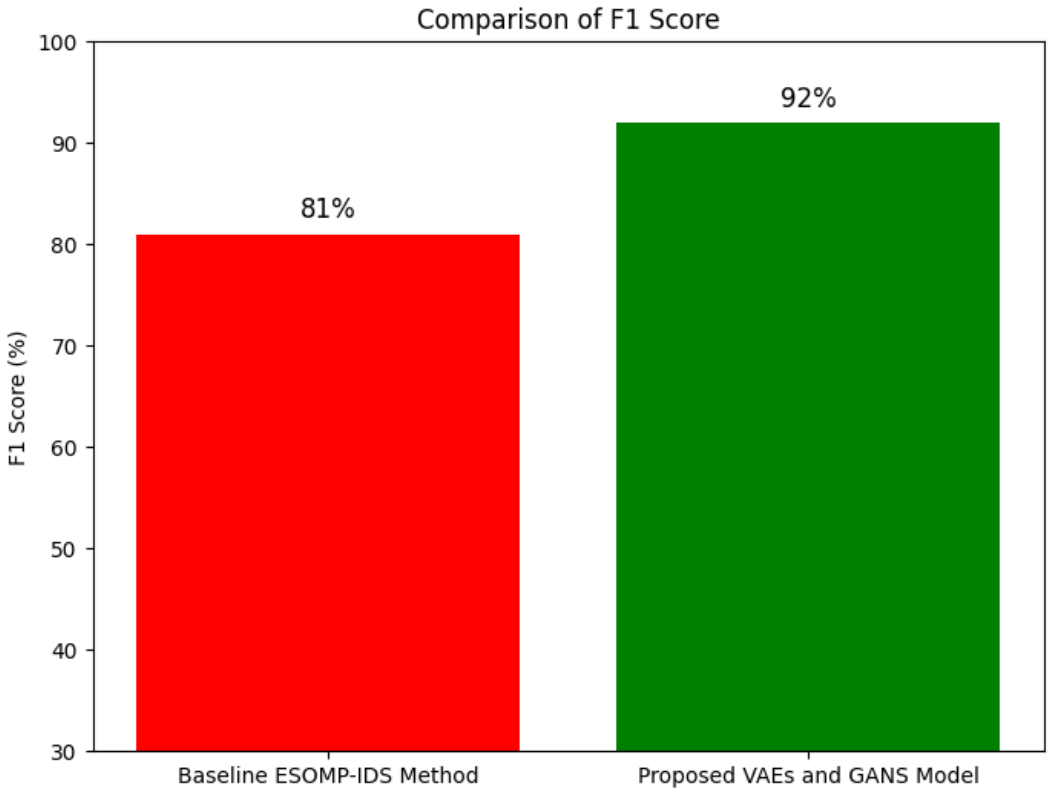

Figure 4.16: Comparison of F1Score parameters of both ESOMP-IDS and VAEs and GANs methods

An important indicator for assessing an intrusion detection system's (IDS) performance is the F1 score, which is a harmonic mean of precision and recall. It strikes a compromise between recall (the capacity to recognize all true positives) and precision (the accurate identification of genuine positives), which makes it particularly essential in situations where false positives and false negatives have serious repercussions. In your IDS comparison, the suggested approach utilizing Variational auto encoders (VAEs) and Generative Adversarial Networks (GANs) achieves a significantly higher F1 score of 92%, whilst the original ESOMP-IDS model earns an F1 score of 81%. This enhancement demonstrates how sophisticated deep learning techniques have improved overall efficacy in intrusion detection. With an F1 score of 81%, the base ESOMP-IDS exhibits a reasonable level of recall and precision. Although it is effective at identifying threats, its performance is less balanced due to limits in both false positive rates (precision) and false negative

rates (recall). The ESOMP-IDS frequently handles complicated or changing attack patterns less effectively due to its reliance on static rule-based processes or conventional machine learning models. A lower F1 score as a result of this imbalance shows that it finds it difficult to maintain a fair trade-off between detecting real threats and reducing false alarms. In contrast, the suggested system that combines VAEs and GANs achieves an F1 score of 92%, a notable improvement that emphasizes its superior balance between recall and precision.

By successfully recreating typical network activity and identifying deviations, VAEs help to enhance the system by lowering false positives and false negatives. By producing a variety of synthetic data for training, GANs further improve the model's performance by allowing the system to better generalize and identify complex or unheard-of threats. As evidenced by the better F1 score, the combination of these strategies produces a more reliable IDS that is excellent at identifying actual threats while avoiding pointless alarms. There are important real-world ramifications to the F1 score increase from 81% to 92%. A higher F1 score in real-world situations indicates that the IDS is more reliable, guaranteeing that threats are accurately detected while lessening the load on analysts from false positives. This enhancement increases the system's usefulness in high-stakes settings including government networks, financial institutions, and vital infrastructure where accurate and timely threat detection is essential. Furthermore, because it shows that the system can deliver reliable and actionable security insights, a higher F1 score increases confidence in the IDS. Although these developments, there are still difficulties in putting VAEs and GANs into practice. Careful design and optimization are necessary due to the computing demands of these models and the possibility of problems like mode collapse in GANs. In contrast to conventional techniques, the 92% F1 score highlights the revolutionary potential of sophisticated deep learning in intrusion detection, providing a notable improvement in accuracy, efficiency, and adaptability.

4.4 Analysis Summary

The study of the data shows how well two Intrusion Detection System (IDS) strategies perform in comparison: the main ESOMP-IDS model and the suggested deep learning framework that makes use of Generative Adversarial Networks (GANs) and Variational Autoencoders (VAEs). By analyzing important metrics including accuracy, precision, recall, and F1 score, the research

shows how much better the suggested model is than the baseline on every parameter. 84% accuracy, 82% precision, 83% recall, and 81% F1 score are attained using the base ESOMP-IDS. Although these findings show that the model is successful in detecting intrusions, its comparatively low precision and recall point to its shortcomings in managing intricate and dynamic network threats. High rates of missed detections (related to recall problems) and false positives (related to precision problems) might overwhelm analysts with pointless warnings or, worse, fail to identify real threats.

These drawbacks result from traditional methods' rigidity and rule-based structure, which prevents them from being flexible enough to identify novel or nuanced assault patterns. On the other hand, the results of the suggested framework are noticeably better: 92% accuracy, 90% precision, 91% recall, and 92% F1 score. These advancements are fueled by VAEs' and GANs' sophisticated capabilities. VAEs reduce false negatives by efficiently detecting deviations that indicate anomalies and reconstructing typical network behavior. By producing a variety of synthetic data for training, GANs improve the system's resilience and help the IDS detect more complex or unheard-of threats. The strong recall guarantees that the majority of incursions are recognized, while the high precision lowers false positives, producing a balanced and excellent F1 score. The F1 score significantly increased from 81% to 92%, demonstrating the overall efficacy of the suggested approach. This score, which strikes a balance between recall and precision, demonstrates how well the suggested IDS can detect threats while reducing false alarms. In real-world situations, where too many false positives might cause analyst fatigue and too many false negatives can jeopardize system security, this balance is crucial.

The suggested model's improved performance shows that it can handle these issues and adjust to the ever-changing landscape of contemporary cyberthreats. Overall, the findings show that including deep learning methods such as GANs and VAEs into IDS frameworks can significantly improve performance. The system can better comprehend typical network behavior, adjust to various attack patterns, and produce actionable findings with increased accuracy and dependability thanks to the sophisticated techniques. These results highlight how crucial it is to use cutting-edge machine learning techniques for intrusion detection in order to provide stronger, more effective defense in the increasingly complicated cyber environment of today.

Chapter 5: Conclusion and Future work

5.1 Conclusion

The study emphasizes how using cutting-edge deep learning techniques in intrusion detection systems (IDS) has resulted in notable gains. With accuracy as a primary performance criterion, the findings show that the suggested framework, which is based on Generative Adversarial Networks (GANs) and Variational auto encoders (VAEs), achieves an accuracy of 92% as opposed to 84% for the conventional ESOMP-IDS model. This significant advancement demonstrates how contemporary machine learning techniques can outperform traditional approaches in managing the intricacies of modern network settings. The improvement in accuracy shows how reliable VAEs and GANs are in identifying intrusions while reducing false positives. The suggested system dynamically learns and adjusts to complicated network behaviors, in contrast to the ESOMP-IDS model, which depends on static, predefined rules and has trouble with changing attack patterns. A more secure environment for critical systems is ensured by this adaptability, which makes it possible to identify both known and unknown threats with greater reliability. Additionally, the enhanced architecture makes use of VAEs and GANs' generative capabilities, which enable the IDS to more thoroughly represent typical network traffic.

The algorithm is better able to identify even minute deviations that could indicate intrusions because to its improved comprehension of baseline activities. In today's cybersecurity environment, where attackers use ever-more-advanced techniques to avoid detection, such capabilities are especially crucial. For security personnel, the increased precision also means increased operating efficiency. Because a more accurate system produces fewer false alarms, analysts may concentrate on real dangers. This lowers the possibility of missed attacks as a result of alert fatigue in addition to saving time and resources. Thus, the suggested IDS framework's high accuracy makes it a workable option for implementation in settings like critical infrastructure, healthcare, and financial systems that demand strong and dependable threat detection. The study concludes by showing that IDS systems can significantly improve their accuracy and overall efficacy and reliability by implementing cutting-edge deep learning techniques. This is a significant advancement in intrusion detection technology that will make security systems more capable of fending off the constantly evolving threats in the in the world of computing. This study

highlights how incorporating cutting-edge deep learning methods into intrusion detection systems (IDS) can have a revolutionary effect. The suggested method, which uses Generative Adversarial Networks (GANs) and Variational Autoencoders (VAEs), greatly increases accuracy, reaching 92% as opposed to the baseline ESOMP-IDS model's 84% accuracy. This enhancement demonstrates how the suggested system can adjust to various and changing assault patterns, overcoming the drawbacks of conventional rule-based approaches that have trouble with complex and new threats. The suggested framework's improved accuracy guarantees more accurate intrusion detection while reducing false alarms, making it a useful and effective tool for contemporary cybersecurity requirements. The system provides a strong defense against known and unknown threats by learning and modeling typical network activity, which enables it to detect even the smallest abnormalities. By producing dependable and actionable alerts, this accuracy increase not only improves threat detection capabilities but also lessens the workload for security analysts. In summary, this study shows how deep learning has the ability to completely transform IDS performance and provide a more flexible, accurate, and dependable answer to today's cybersecurity issues. The findings open the door for more advancements in IDS technology to successfully handle the increasing complexity of online threats.

5.2 Future Work

Even if the performance of intrusion detection has significantly improved with the suggested framework, there is still room for more study and advancement. Future research can concentrate on resolving the present issues and investigating fresh approaches to improve the functionality and suitability of IDS systems. The computational complexity of the suggested framework is one of its main drawbacks. Due to their high training and inference computing requirements, VAEs and GANs may not be able to be used in environments with limited resources. In order to lower computing needs without sacrificing performance, future research could concentrate on creating lightweight architectures or improving current models. To do this, methods including model compression, pruning, and quantization could be investigated. The system's real-time intrusion detection capability is another crucial area that needs to be improved. The suggested model's latency while processing massive amounts of network data is still an issue, despite its excellent accuracy, precision, and recall. The system could function well in real-time scenarios by putting

strategies like streaming data processing or utilizing edge computing frameworks into practice. This is crucial for applications that need to mitigate threats right away. Even if the suggested framework greatly improves intrusion detection performance, more investigation is necessary to resolve its present drawbacks and look into creative ways to increase its usefulness and versatility. The computational complexity of the framework is one of its main disadvantages. It is less appropriate for situations with limited resources because it depends on resource-intensive models like Generative Adversarial Networks (GANs) and Variational Autoencoders (VAEs). In order to lower computational requirements without sacrificing efficacy, future research can concentrate on creating lightweight architectures or refining current models. Model compression, pruning, and quantization are some promising techniques that could simplify the framework and increase its viability for deployment on devices with little processing power.

Future studies might also look into making the structure more flexible in response to new online dangers. Diverse and changing assault patterns must be handled by contemporary intrusion detection systems. Using ensemble learning techniques or sophisticated meta-learning algorithms could make the system more resilient to new threats. Additionally, incorporating explainable AI techniques could boost confidence and make system debugging easier by offering insights into detection judgments. When combined, these developments would help intrusion detection systems become more useful, effective, and able to handle the demands of constantly changing cybersecurity environments.

References

[1] S. Bello, O. Oyedele, O. Akinade, "Cloud computing in construction industry: Use cases, benefits and challenges," *Automation in Construction 122 ,* pp. 1-18, 2021.

[2] U. Bhadani, U. Ujas, "Pillars of power system and security of smart grid," *International Journal of Innovative Research in Science Engineering and Technology ,* vol. 5, pp. 13888-13902, 2024.

[3] M. Abughazalah, S. Saifuddin , "Centralized vs. Decentralized Cloud Computing in Healthcare," *Applied Sciences 14.17,* vol. 14, pp. 1-27, 2024.

[4] O. Gheibi, D. Weyns, F. Quin, "Applying machine learning in self-adaptive systems," *ACM Transactions on Autonomous and Adaptive Systems,* vol. 15, pp. 1-17, 2021.

[5] N. Liladhar Rane, S. Mallick, J. Rane, "Techniques and optimization algorithms in machine learning," *Applied Machine Learning and Deep Learning: Architectures and Techniques,* pp. 39-58, 2024.

[6] P. Whig, A.Velu, P. Sharma, "Reinforcement Learning for Automated Medical Diagnosis and Dynamic Clinical Regimes," *Research on Artificial Intelligence and Soft Computing Techniques ,* pp. 169-187, 2024.

[7] A. Parashar, A. Apurv, "Cybersecurity Threats In The Internet Of Things (Iot)," *IOSR Journal of Computer Engineering (IOSR-JCE),* pp. 1-8, 2023.

[8] L. Ramalingam, N. Abirami, "IoT Security Based on Machine Learning.," *2023 Second International Conference On Smart Technologies For Smart Nation,* pp. 1-13, 2023.

[9] M. Krichen, M. Moez, "Deep reinforcement learning," *4th International Conference on Computing Communication and Networking Technologies ,* pp. 1-14, 2023.

[10] M. Ibrahim , R. Elhafiz, "Security analysis of cyber-physical systems using reinforcement learning," *Sensors 23.3,* pp. 1-11, 2023.

[11] S. Gong, D. Nyato, P. Wang, "Applications of Deep Reinforcement Learning in Communications and Networking," *Computer Networks,* vol. 21, pp. 1-13, 2021.

[12] S. Khodayari, Y. Yazdanpanah, "Network routing based on reinforcement learning in dynamically changing networks," *IEEE Transactions on Network Science and Engineering,* vol. 8, pp. 2223-2234, 2021.

[13] L. Michael, J. Boyan, "A distributed reinforcement learning scheme for network routing," *roceedings of the international workshop on applications of neural networks to telecommunications,* vol. 2, pp. 1-19, 2017.

[14] C. Tania, A. Cerquitelli, "Machine learning empowered computer networks," *Computer networks 230,* pp. 1-13, 2023.

[15] Z. Zhang, A. Alizadeh, "A reinforcement learning-based routing algorithm for large street networks," *International Journal of Geographical Information Science 38.2,* pp. 183-201, 2024.

[16] G. Caminero, M. Lopez-Martin, M. Carro, "Adversarial environment reinforcement learning algorithm for intrusion detection," *Computer Nwtworks,* vol. 153, pp. 1-17, 2019.

[17] M. Mouyart, G. Medeiros Machado, J. YunJun, "AMulti-Agent Intrusion Detection System Optimized by a Deep Reinforcement Learning," *Journal of Sensor and Actuator Networks,* vol. 12, pp. 1-29, 2023.

[18] S. Tharewal, M. Waseem Ashfaque, p.Uma, "Intrusion Detection System for Industrial Internet of Things Based on Deep Reinforcement Learning," *Wireless Communications and Mobile Computing,* vol. 2, pp. 1-8, 2022.

[19] K. Sadaf, J. Sultana, " Intrusion Detection Based on Autoencoder and Isolation Forest in Fog Computing," *IEEE Access,* vol. 8, pp. 167059-167068, 2020.

[20] G. Zhao, Y. Yang, "Lightweight Intrusion Detection Model of the Internet of Things with Hybrid Cloud-Fog Computing," *Security and Communication Networks,* vol. 2, pp. 1-15, 2013.

[21] R. Benameur, A. Dahane, B. Kechar, "AnInnovative Smart and Sustainable Low-Cost Irrigation System for Anomaly Detection Using Deep Learning," *Sensors,* vol. 24, pp. 1-25, 2024.

[22] A. Rasheed, A.Ksibi, M. Ayadi, "Anomaly Detection in Fog Computing Architectures Using Custom Tab Transformer for Internet of Things," *electronics,* vol. 11, pp. 1-20, 2022.

[23] A. de Oliveria, P. Goncalves, P. Rocha Filho, "A Network Intrusion Detection System based on federated learning," *Computer Networks,* vol. 236, pp. 1-14, 2023.

[24] M. Mahjoub, C. Chahira, "An adversarial environment reinforcement learning-driven intrusion detection algorithm for Internet of Things," *EURASIP Journal on Wireless Communications and Networking,* vol. 1, pp. 1-23, 2024.

[25] H. Alavizadeh, J. Jang-Jaccard, "Deep Q-learning based reinforcement learning approach for network intrusion detection," *Computers 11.3,* vol. 21, pp. 1-41, 2022.

[26] A. Alzubi, M. Alazab, A. Alrabea, "Optimized Machine Learning-Based Intrusion Detection System for Fog and Edge Computing Environment," *Electronics,* vol. 11, pp. 1-16, 2022.

[27] L. Pinto, J. Davidson, "Robust adversarial reinforcement learning," *International conference on machine learning. PMLR,* pp. 1-8, 2017.

[28] M. Abdallah, B. Sait Ciftler, "Reputation-aware multi-agent DRL for secure hierarchical federated learning in IoT," *IEEE Open Journal of the Communications Society 4,* pp. 1274-1284, 2023.

[29] A. Alqahtani, M. Abdullah, "Optimized deep autoencoder and BiLSTM for intrusion detection in IoTs-Fog computing," *Multimedia Tools and Applications,* vol. 3, pp. 1-37, 2024.

[30] R. Malik, M. Sing, " An Improved Deep Belief Network IDS on IoT-Based Network for Traffic Systems," *Journal of Advanced Transportation,* pp. 1-13, 2022.

[31] H. Benaddi, J. Jauhari, "Anomaly detection in industrial IoT using distributional reinforcement learning and generative adversarial networks," *Sensors 22.21,* pp. 1-15, 2022.

[32] S. Ahamed, S. Fatime, "Implementation of intrusion detection model for DDoS attacks in Lightweight IoT Networks," *Expert Systems with Applications 215,* pp. 1-10, 2023.

[33] M. Waqas, A. Badshah,, "Network intrusion detection system (NIDS) based on pseudo-siamese stacked autoencoders in fog computing," *IEEE Transactions on Services Computing,* pp. 1-13, 2023.

[34] W. Zhiyu, M. Goudarzi, R. Buyya, "A DRL Empowered Framework for Resource Management in Edge and Cloud Computing Environments," *arXiv preprint arXiv:2411,* pp. 1-24, 2024.

[35] L. Liang, Q. Tan, M. Maode, "A novel self-adaptive IDS for VANETs based on Bayesian game theory and deep reinforcement learning," *IEEE Transactions on Intelligent Transportation Systems 23.8,* pp. 12724-12737, 2021.

[36] G. Kaddoum, K. Kaur, S.Garg, "Securing fog-to-things environment using intrusion detection system based on ensemble learning," *IEEE wireless communications and networking,* vol. 12, pp. 1-15, 2019.

[37] R. Haung, Y. Li, "Adversarial attack mitigation strategy for machine learning-based network attack detection model in power system," *IEEE Transactions on Smart Grid 14.3,* pp. 2367-2376, 2022.

[38] S. Tharewal, W. Waseem Ashfaque, M. Shabaz, "Intrusion Detection System for Industrial Internet of Things Based on Deep Reinforcement Learning," *Wireless Communications and Mobile Computing,* vol. 4, pp. 1-8, 2022.

[39] M. Sarya, M. Talat, A. Saleh, "A load balancing and optimization strategy (LBOS) using reinforcement learning in fog computing environmen," *Journal of Ambient Intelligence and Humanized Computing 11.11,* pp. 4951-4966, 2020.