NAVIGATING CYBERSECURITY: A COMPREHENSIVE ANALYSIS OF MACHINE LEARNING IN CYBER ATTACK DETECTION

S. DEEPA RAJAN[1*], A. MANIKANDAN[2]

[1, 2]Department of Computer Science and Engineering, Vels Institute of Science, Technology and Advanced Studies, VISTAS, Chennai, Tamil Nadu.

Email: [1]deepasdinesh@gmail.com, [2]mani.se@velsuniv.ac.in

ABSTRACT

In the ever-evolving landscape of cyber threats, the integration of machine learning (ML) techniques has emerged as a powerful tool for detecting and mitigating attacks across various sectors, such as the Internet of Things (IoT) and Wireless Sensor Networks (WSN). This analysis paper examines several ML algorithms, such as Random Forest (RF), Ridge Classifier, and Gaussian Naive Bayes, and their efficacy in enhancing cyber-attack detection accuracy and efficiency. Emphasising the significance of preprocessing data and feature extraction, our paper highlights the exceptional performance of hybrid models and the transformative role of Multi-Agent Reinforcement Learning (MARL) in addressing the challenges posed by class imbalance and rapidly evolving threats. This paper underscores the critical need for continuous innovation in cybersecurity measures by showcasing the promising results achieved through these techniques. Ultimately, our findings reveal that while various ML approaches have successfully detected cyber-attacks, the implementation of MARL represents a significant advancement in developing robust and adaptive intrusion detection systems.

Keywords: *Cyber-Attack, Machine-Learning, Multi-Agent Reinforcement Learning, Cyber-Security, Intrusion Detection System.*

1. INTRODUCTION

In today's hyper-connected world, cyber-attacks have escalated into a growing concern, impacting individuals, organizations, and governments globally. These attacks have evolved in scale, complexity, and sophistication, often leading to devastating consequences across various sectors. Cyber-attacks are malicious attempts to compromise digital assets' confidentiality, integrity, or availability, with adversaries frequently targeting sensitive data, critical systems, and infrastructure [1]. The tactics attackers use are wide-ranging, exploiting vulnerabilities in computer systems, networks, and applications. Common cyber-attacks include data breaches, ransomware, distributed denial-of-service (DDoS) attacks, and phishing scams [2]. These attacks can have multiple motivations, such as financial gain, espionage, sabotage, activism, and cyber warfare. Regardless of the motivations, cyber-attacks have serious consequences, including significant economic losses, reputational damage, disruption of essential services, and severe risks to public safety [3].

To counter these persistent and evolving cyber threats, Intrusion Detection Systems (IDS) have emerged as a necessary component in ensuring the security of information systems [4]. IDS solutions identify and mitigate unauthorised or malicious activities in real time, providing a critical defence against cyber intrusions [5]. These systems continuously monitor network traffic, system logs, and various data sources to detect suspicious patterns, anomalies, or known attack signatures. IDS are generally categorized into three forms: network-based IDS (NIDS), host-based IDS (HIDS), and hybrid systems that incorporate both NIDS and HIDS [6]. NIDS monitor network traffic for potential threats, while HIDS detect malicious activity on individual devices or hosts [7].

This study focuses specifically on the integration of Multi-Agent Reinforcement Learning (MARL) within the context of IDS for the Internet of Things (IoT) and Wireless Sensor Networks (WSN). It delves into the potential of MARL to enhance detection accuracy, adapt to evolving cyber threats, and address challenges such as class imbalance. However, this study does not cover the implementation details of specific algorithms or explore all possible machine-learning techniques available for IDS. Additionally, it does not address the physical security aspects of IoT and WSN environments, focusing solely on the digital and algorithmic dimensions of cyber security.

This study's limitations include relying on existing datasets to evaluate the effectiveness of the proposed MARL approach, which may not fully capture the dynamic nature of real-world cyber threats. Furthermore, the study does not consider the hardware or software constraints that may affect the deployment of MARL-based IDS in practical scenarios. While this research aims to provide insights into improving intrusion detection through MARL, future studies will be necessary to validate these findings in diverse environments and with broader datasets.

As cyber-attacks become more distributed and dynamic, the need for advanced methodologies has become apparent [8]. One such advancement is the exploration of MARL, which introduces a decentralized and adaptive approach to enhancing IDS capabilities [9]. MARL distributes detection responsibilities across multiple agents, each assigned to monitor different aspects of a network or system, allowing for more comprehensive and scalable threat detection [10]. Each agent in a MARL framework is trained to focus on specific tasks or areas within a system and works collaboratively with other agents to identify and respond to threats that may exhibit complex or evolving behaviours [11].

The collaborative nature of MARL introduces collective intelligence, where agents share information, thus enhancing the system's overall capability to detect and respond to cyber-attacks [12]. Moreover, MARL enables these agents to learn from environmental feedback, continuously refining their detection strategies as cyber threats evolve [13]. By leveraging this learning capability, MARL adapts in real-time, significantly improving detection accuracy and efficiency compared to traditional IDS [14]. This adaptability allows the system to respond effectively to emerging threats constantly changing in nature, making MARL-based IDS an essential tool in the modern cybersecurity landscape.

By introducing real-time adaptability and decentralization, MARL substantially increases the resilience of cybersecurity systems. The dynamic and distributed nature of MARL-based IDS solutions allows organizations to handle the growing complexity of cyber threats, providing a scalable solution capable of addressing attacks in distributed and multi-layered networks [15]. MARL not only increases the accuracy of intrusion detection but also provides a robust framework for scaling security efforts as networks become complex. This adaptability is essential as cyber adversaries evolve tactics, finding new ways to bypass traditional defence [16]. MARL's dynamic capabilities make it a promising framework for future cybersecurity systems, offering intelligent and proactive defence mechanisms that can keep pace with the challenges posed by ever-evolving cyber adversaries.

Ultimately, MARL's application in cybersecurity opens up new avenues for developing intelligent and autonomous defence systems that can operate effectively in complex, fast-changing environments [17, 18]. As cyber threats increase in both volume and sophistication, future research and development efforts will likely focus on further optimizing MARL frameworks for practical implementation, ensuring that these advanced systems can meet future security needs.

The contributions of this analysis are as follows:

- The integration of the RF algorithm within the Feedzai platform significantly enhanced real-time fraud detection, showcasing ML's potential in mitigating financial cyber threats.
- The Ridge Classifier-based IoT security system achieved high accuracy, emphasizing the importance of feature extraction in predicting cyber-attacks and enhancing IoT network security.
- Gaussian Naive Bayes and SGD, combined with PCA for feature selection, improved intrusion detection in WSNs, demonstrating the value of dimensionality reduction in IDS performance.
- The hybrid model combining ML and AI techniques with K-Means Clustering achieved outstanding accuracy, underscoring the effectiveness of data balancing and hybrid approaches in cyber-attack detection.
- The MARL architecture addressed traditional IDS limitations, offering a more adaptive solution to class imbalance and evolving threats, with high detection accuracy across various attack types.

This structured approach helps highlight the strengths and limitations of different cyber-attack detection techniques and provides valuable insights into the most efficient methods for enhancing cybersecurity resilience. Section 2 offers an overview of the existing literature and identifies key limitations in current methodologies. Section 3 explores a detailed analysis of studies related to cyber-attack detection in various domains. A comparative investigation of the performance of various techniques is presented in Section 4, with Section 5 providing an in-depth discussion of the findings. Section 6 summarises the paper's main contribution and future research directions, followed by references.

2. LITERATURE SURVEY

Zachariah et al. [19] addressed the challenge of classifying cyber-attacks by utilizing both RF and Artificial Neural Network (ANN) techniques. The study was based on the widely-used CICIDS2017 dataset, which provides a comprehensive collection of intrusion detection data. The authors employed the Boruta feature selection method to enhance the classification performance, a robust algorithm designed to identify all relevant variables within a dataset. The selected features aimed to reduce computational complexity while improving classification accuracy. By comparing the two models' performances, the research offers important new information on how well ML approaches work to recognise cyber-attacks. But it's possible that the dataset doesn't accurately reflect how cyberattacks are changing in real-world scenarios.

Roopa et al. [20] proposed a cyber-attack recognition model for IIoT employing a Voting-Based Ensemble method, combining classic and modern ML algorithms like Histogram Gradient Boosting, CatBoost, and RF. The framework employs a hard voting classifier to enhance the detection efficiency of cyber-attacks, with CatBoost achieving the highest accuracy compared to the other algorithms. However, the reliance on specific algorithms may reduce the framework's adaptability to diverse datasets or evolving attack patterns, potentially affecting its generalizability in different IIoT environments.

Information security professionals have recently become more interested in the concept of hybrid learning for strengthening defences against CT. In the work of Mohammed Naif et al. [21], a hybrid approach combining swarm intelligence and evolutionary algorithms for feature selection, PSO-GA (Particle Swarm Optimization-based Genetic Algorithm), was applied to the CICIDS-2017 dataset. The method was assessed by employing an Extreme Learning Machine (ELM) combined with Bootstrap Aggregation (ELM-BA) to enhance the success rate of the ELM. This approach attains a maximum reliability rate, demonstrating its effectiveness in cybersecurity applications. However, further evaluation of additional datasets will enhance their performance and generalizability.

Baha et al.[22] highlighted anomaly-based detection as a common approach in intrusion detection systems, focusing on identifying abnormal patterns indicative of malicious activities. They explored various machine learning techniques, noting that many datasets used for evaluation do not fully represent real-world network traffic, leading to challenges in model generalization. Their analysis focused on CICIDS2017, which mirrors modern network environments, and NSL-KDD, an improved KDD'99 dataset. Using stacking, they developed a hybrid model combining decision trees and random forest algorithms. However, a limitation is the reliance on datasets that may not fully capture real-world traffic complexity.

Birnur et al.[23] suggested an approach to improve the outcomes of IDS by focusing on multivariate outlier detection and optimal feature selection. The 41-feature NSL-KDD dataset was employed in the system's creation and testing. Initially, the ReliefF approach was used to reduce the feature set to 20 key features while maintaining high classification performance. The RF approach emerged as a top performer, attaining high accuracy and outperforming other techniques. The approach's reliance on the NSL-KDD database may limit its applicability to more modern and real-world network environments.

Yusuf et al. [24] focused on developing ML-based IDS to address the increasing vulnerability of growing network traffic. The study used the CICIDS2017 dataset containing recent and historical attack data and applied ML models. The dataset was pre-processed through cleaning, normalization, oversampling for imbalanced labels, and feature selection to improve model performance. A high-performance computer was utilised for rapid testing. Among the classifiers, random forest showed the highest accuracy. Despite the positive results, the approach requires continuous updates to the dataset to reflect evolving real-world cyber threats.

Said et al.[25] developed a hybrid NIDS that integrates both SNIDS and ADNIDS methodologies. The model is designed to identify various types of CT, such as zero-day intrusions and exploits, leveraging the open-source Suricata system alongside ML systems. The Decision Tree algorithm demonstrated impressive performance in classifying benign traffic, achieving an impressive accuracy rate. The current model has yet to be fully optimized, as it has only been tested with a single algorithm and dataset, which may limit its generalizability and effectiveness in diverse environments.

This literature survey highlights various approaches to improving cyber-attack detection, including ML algorithms and hybrid models that integrate multiple classifiers. Studies emphasised the importance of feature selection techniques in enhancing classification performance and reducing computational complexity. However, many proposed models face limitations in generalizability due to reliance on specific datasets and algorithms, necessitating further evaluation of diverse and real-world data.

2.1 Problem statement

Despite the increasing use of ML techniques for cyber-attack detection, significant hurdles remain in ensuring the models' effectiveness and adaptability in real-world circumstances. Many recent studies rely on specialized datasets, such as CICIDS2017 and NSL-KDD, that may not correctly reflect the changing nature of cyber threats and real-world network traffic complexities. Furthermore, while hybrid models have shown promise in improving detection performance, their generalizability across different environments and flexibility to evolving assault patterns are still limited. This emphasizes the need for novel methodologies that increase detection accuracy and adapt to the ever-changing landscape of cyber threats.

To address these challenges, this research aims to explore the following research questions:

1. How can hybrid models be developed to improve the accuracy of cyber-attack detection while remaining adaptable to various datasets and changing threat landscapes?
2. What role may sophisticated approaches like MARL play in combating class imbalance and rapidly changing attack patterns in cyber-attack detection systems?
3. How can integrating varied datasets enhance the training and performance of machine learning-based intrusion detection systems, ensuring their efficacy against a broader spectrum of cyber threats?
4. What preprocessing and feature selection techniques may be used to improve the performance of ML models in cyber-attack detection, and how do they affect model robustness?

3. ANALYSIS OF ML TECHNIQUES FOR CYBER ATTACK DETECTION ACROSS DIVERSE DOMAINS

Cyber-attack detection using ML techniques has become vital to enhancing cybersecurity measures. ML automatically identifies patterns and anomalies within network traffic and system behaviour by leveraging advanced algorithms. These techniques facilitate the detection of numerous forms of CT containing malware, phishing, and intrusion attempts. Additionally, ML techniques enhance their efficacy by assimilating fresh data, rendering them flexible enough to adjust to changing attacking ways. This proactive approach enhances detection accuracy and significantly reduces response times to potential security breaches.

3.1. Cyber threat detection and mitigation strategies using Random Forest algorithm [26]

This study investigates methods for identifying and countering next-generation CT, focusing on the functions of artificial intelligence (AI) and machine learning (ML). It provides how these technologies contribute to cybersecurity, particularly in fraud detection and prevention systems. Additionally, it provides views into the approaches' revolutionary potential and shows the advantages of incorporating them into cyber security operations. The specific focus of this research is the efficacy of combining AI and ML methods with the Feedzai security system to improve the identification of criminal activity in banking systems.

This research focuses on utilising AI-based solutions to enhance fraud detection in the financial sector. Feedzai, an intelligent security platform, was integrated with ML techniques, specifically the RF algorithm, to attain precise transaction recognition and identify fraudulent activities in real-time. To verify their approach, the researcher utilised a supervised ML-based RF approach on a dataset of historical transaction records in CSV format. The following steps outline the procedure for detecting anomalies in cyber activities using the proposed Feedzai system:

- The system collects information from various sources, such as network traffic, logs, and security events. The gathered data is then processed through an RF algorithm that assesses and inspects data for potential cyber-attacks.
- The system checks for malicious activities based on the output of the RF algorithm. If malicious activity is detected, further analysis is conducted. The system proceeds to the next stage if no malicious behaviour is identified.
- If an anomaly is detected, the system sends a CT alert to the right persons. Finally, the system logs the CT incident, and the progression is finished.

The Feedzai software tool is implemented in this research to detect anomalies in cyber activities. Recognized as a leading intelligent platform, Feedzai employs AI to effectively identify and stop fraud, especially in the financial industry. Through AI frameworks, Feedzai's powerful anomaly detection technology can recognise patterns and behaviours that could be hard for people to notice. This feature protects financial institutions and their clients from security breaches and monetary losses by enabling the tool to identify and stop criminal activity. The procedure for utilizing ML frameworks within the Feedzai system is as follows:

- The system starts by collecting clients' transaction data and examining their profiles and history.
- External data sources are integrated to enhance the quality of collected data using Feedzai's data consolidation capabilities. ML frameworks monitor and assess transaction risk factors, identifying patterns indicative of financial crime.
- The RF model is employed to combat risks and detect the presence of fraudulent transactions.

The aim of this stage is to consolidate and streamline the financial interactions that the model processes, making it possible to regulate and oversee the fraud detection mechanism effectively. The case manager can observe the real-time rating operations and the forecasts provided by the model for each transaction by pushing these transactions to the front. To ensure a proactive strategy for fraud control, this well-organized listing is a useful resource for carrying out additional analysis, looking into suspicious activity, or acting on transactions that have been identified.

This work evaluates the reliability rates of various CT recognition approaches, specifically ML algorithms. The reliability rate denotes the proportion of CT that each model accurately detects. The results indicate that the RF model attains a maximum success rate of 83.94%, demonstrating its superior effectiveness in detecting cyber-attacks. This effectiveness is explained by RF's capacity to recognize intricate correlations among characteristics, making it very useful for fraud prevention and anomaly identification jobs.

3.2 Security Mechanism to detect and prevent Cyber-attack in IoT networks [27]

In the rapidly expanding IoT landscape, comprehensive protection against network threats is critical. The deployment of robust ML models is essential for detecting and mitigating cyber-attacks in real time. This research develops an ML-based security system using the Ridge Classifier to detect anomalies and forecast CT in IoT systems. Integrating multiple security mechanisms enhances the capacity to recognize and mitigate threats effectively, ultimately contributing to the security of government and business networks.

The primary goal of this research is to create ML-based security processes tailored for IoT environments. These steps are intended to reduce the risks to the network, improve general network security, and guarantee data security. The research utilizes the UNSW-NB15 dataset to assess multiple machine learning techniques, such as ensemble learning, Ridge Classifier, and linear regression, emphasising recognising anomalies in the Internet of Things networks. The dataset serves as the basis for additional evaluation by capturing device actions, network behaviour, and potential risks.

- The unprocessed data is cleaned and formatted appropriately for ML through pre-processing. To assure accuracy in the following analysis, this stage includes removing noise from the data, addressing missing values, normalizing the data, and other crucial data preparation tasks.
- Important elements that indicate traits and trends related to CT are removed from the preprocessed data. Choosing feature approaches are employed to determine which features are most useful and necessary for precise threat recognition.
- Various ML models are assessed to determine which algorithm is best for detecting threats. The Ridge Classifier was selected for this investigation due to its accuracy in detecting anomalies and its resilience while working with huge datasets. Neural networks, RF, and decision trees were among the other models considered.
- A labelled dataset comprising daily and potentially dangerous occurrences was used to train the chosen Ridge Classifier model. The model gains the ability to recognize data patterns that point to security threats. A different validation dataset, employing performance measures, was used to assess the trained model.
- After deployment, the trained model analyzes incoming data from IoT devices and network logs in or almost real-time. Observed patterns are compared with taught patterns to identify potentially harmful or suspicious activity.
- The system starts the necessary security steps to reduce the risk when it detects a threat. IDS activation, network or device isolation, traffic blocking, isolating impacted devices, and notifications for additional research are a few examples of these preventative measures.
- The Ridge Classifier demonstrated exceptional performance in detecting cyber-attacks

within IoT systems. The system obtains a notable accuracy rate of 97%, with precision at 98.3%, recall at 98.5%, and an F1-score of 98.4%. These results indicate the Ridge Classifier's effectiveness in identifying threats and mitigating network risks in real time.

The findings highlight the significance of using ML models like the Ridge Classifier in IoT security. The suggested approach improves the security and resilience of corporate and governmental networks by precisely identifying threats and implementing real-time security measures. Various security procedures enhance the defence against various CTs, safeguarding precious data and promoting trust in Internet of Things devices.

3.3 ID in WSN using Stochastic Gradient Descent technique [28]

Communication within CPS relies heavily on WSNs, which are employed for various tasks such as ambient monitoring, object recognition, and data transmission. The integration of WSNs with the IoT exposes these networks to numerous cyber-attacks. To address the challenges associated with WSN ID, this research explores the use of ML techniques, particularly focusing on the Gaussian Naive Bayes (GNB) and SGD algorithms.

The study addresses the computational challenges of IDS, which often struggle with processing large volumes of network data, resulting in performance issues. Singular value decomposition (SVD) and PCA are two feature selection techniques that minimise the dimensionality of the data without sacrificing crucial information to optimise this process. This decrease in processing complexity makes more efficient ID possible.

- ➢ The high computational expense of traditional WSN intrusion detection systems often stems from the large amount of data that needs to be processed. To tackle this, feature selection methods such as PCA and SVD were employed to reduce the dimensionality of the dataset while retaining crucial data. These pre-processing methods lighten the IDS's computational load while improving the categorizing technique's overall recognition reliability.
- ➢ The SG-IDS model was developed by comparing the performance of GNB and SGD classification strategies on the WSN dataset. The goal was to detect network traffic anomalies and cyber-attacks with fewer false positives, overcoming the limitations of traditional WSN intrusion detection methods, such as poor detection accuracy and slow real-time performance.
- ➢ The study utilized the WSN-DS dataset and the WUSTL EHMS 2020 dataset as input data, with intrusion classifications as the output. To streamline the detection process, the model incorporated hyperparameters such as the learning rate and the number of iterations for the SGD algorithm.
- ➢ The dataset was split into 70% training and 30% testing sets. The models were trained separately using GNB and SGD. The final evaluation yielded an accuracy of 0.98, a precision of 0.96, a recall of 0.97, and an F1 score of 0.96.

The overall results of this study highlight the significance of integrating advanced ML models such as SG-IDS for real-time ID in WSNs. The proposed system achieves high accuracy rates in securing WSN-based IoT environments, contributing to the broader efforts to enhance the resilience and security of CPS networks. The findings emphasize the need to continuously improve and adapt ML-based intrusion detection systems to mitigate evolving cyber threats.

3.4 Cyber-attack detection in WSN using hybrid feature reduction and k-means clustering algorithm [29]

The application of AI in detecting cyberattacks within WSNs involves utilizing a hybrid feature reduction technique to create a system capable of efficiently identifying and classifying cyberattacks in WSN environments. This work presents an intelligent hybrid model designed to improve the defence of WSNs by detecting and preventing cyber-attacks. The suggested model integrates ML and AI techniques, utilizing various feature reduction methods, clustering models, and deep learning algorithms to achieve optimal performance.

- The model processes features extracted from network traffic data in the WSN environment. These features include packet headers, traffic patterns, and other relevant attributes. Feature reduction techniques are employed to handle the large volume of traffic data and retain essential information. These techniques help reduce the dimensionality of the dataset while preserving the key features associated with various attack types.
- Once feature reduction is complete, the model applies a K-Means Clustering Model enhanced by Information Gain (KMC-IG). This step further refines the dataset by clustering similar behaviours and patterns, facilitating better classification during the ID process. Information Gain is applied to rank and prioritize the features based on their contribution to the classification task,

thereby improving the overall efficiency of the model.

- The Synthetic Minority Excessively Technique is introduced to address imbalances in the dataset between the majority and minority classes. This approach creates synthetic instances of minority class samples, ensuring a balanced dataset. This step is needed to enhance the models' ability to handle underrepresented attack types and reduce false positives in intrusion detection.
- The Deep Feed-Forward Neural Network (DFNN), specifically made for ID and network traffic classification in WSNs, is the central component of the suggested model. The DFNN architecture has three layers: input, hidden, and output. Applying activation functions such as Rectified Linear Unit (ReLU) among layers allows for the introduction of non-linearity and the capture of intricate patterns in the data.
- The models' effectiveness is assessed on three well-known datasets (NSL-KDD, UNSW-NB15, and CICIDS 2017) using conventional measures like accuracy, precision, recall, and F1-score. Two scenarios—complete feature sets and the other with reduced feature sets—are used for the evaluation. On the NSL-KDD dataset with decreased features, the SG-IDS model performs exceptionally well, attaining a high accuracy of 99%, recall of 97.8%, F1-score of 98.8%, and precision of 99%.
- The DLFNN-KMS-IG model is compared against other benchmark ML algorithms to validate its superiority in intrusion detection for WSN environments. The results indicate that the proposed model outperforms traditional models, especially in accuracy, demonstrating its effectiveness for early detection and real-time protection against cyber-attacks.

The study concludes that the proposed intelligent hybrid model effectively enhances WSN security by integrating SVD, PCA and KNMC-IG with a DL-based DFNN for intrusion detection. The model reduces computational complexity and achieves high accuracy and precision in detecting a wide range of cyber-attacks. The research highlights the importance of feature reduction and data balancing techniques for building efficient ML-based security systems that safeguard WSNs from cyber threats.

3.5 Network Intrusion Detection Using Multi-Agent Reinforcement Learning [30]

IDS was crucial in safeguarding computer networks from various cyber threats. Because ML techniques can evaluate and discover patterns from vast datasets, they have been extensively utilised for IDS. However, the advent of new attack types and the rapid evolution of attack patterns have made it difficult for existing ML-based IDS solutions to stay up. These systems also had to deal with issues of class imbalance, where certain classes (such as particular attack kinds) were underrepresented, which made it harder to identify these lesser classes.

In response to these challenges, a novel MARL architecture was proposed in this work, offering automatic, efficient, and robust intrusion detection in network environments. The architecture built upon and improved the traditional Deep Q-Network (DQN) algorithm by integrating the weighted mean square loss function and employing cost-sensitive learning techniques. These enhancements were tailored to address the class imbalance problem and improve detection accuracy. This work proposed a novel approach for intrusion detection utilizing a MARL framework. This solution employed a two-level structure, as shown in Figure 1. The first level, referred to as the detection level, consisted of multiple independent RL agents (L1 agents), each designed to detect a specific type of attack. These L1 agents could take three possible actions: detecting a target attack, detecting other types of attacks, or identifying normal traffic. All L1 agents shared the same state, representing the network traffic's relevant characteristics. The second level of the framework involved a single decider agent that received input from the L1 agents and was responsible for making the final classification. The decider agent had a set of possible actions, including identifying any attack or recognizing normal traffic. This architecture was designed to be flexible and capable of evolving over time. New attacks could be incorporated by adding a new L1 agent for the specific attack type and retraining the decider agent. The system could also handle changes in attack patterns by retraining the relevant L1 agent and the decider agent for a limited number of episodes.

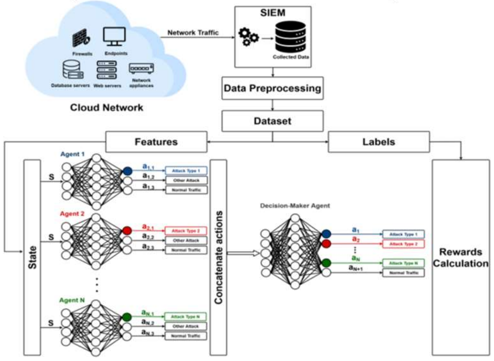


Figure 1: MARL intrusion detection system architecture [30]

A security Information and Event Management (SIEM) system collected data from various cloud network sources. Preprocessing was performed to clean and normalize the raw data, transforming it into usable information. The dataset was divided into a feature set and corresponding labels during the training process. The feature set represented the state of the L1 agents, and the labels were used to calculate rewards by comparing the agents' outputs to the current label.

The training began by initialising the neural network with random weights and the replay memory with a specified capacity for all agents, including the decider agent. The replay memory stores the agents' experiences, later used to train the neural network. For each training episode, L1 agents were trained on all dataset samples. The current state was initialised for each record, representing the feature set, and an action was selected using the ϵ-greedy exploration strategy. Initially, the exploration factor ϵ was set to 1 to encourage random action selection, gradually decreasing to 0 as the agent learned the environment. Rewards were calculated by comparing the selected action with the current state's label, and each experience (state, action, reward) was stored in the replay memory. A random minibatch of these experiences was then selected to update the neural network. The state space, action space, and reward functions for the L1 agents and the decision-maker agent were defined as follows:

State Space (S): All L1 agents shared the same state, which consisted of dataset features. The decider agent's state was composed of the outputs (Q values) generated by the L1 agents for each type of traffic: target attack, other attacks, and normal traffic. These outputs were concatenated to form the decider agent's state vector.

Action Space (A): Each L1 agent had three possible actions: classifying the traffic as its target attack, identifying other attacks, or marking it as normal traffic. The decider agent's action space included one action for each attack type and one for normal traffic.

Reward (R): L1 agents received rewards based on classification accuracy. Positive rewards were assigned for correct classifications, while negative rewards were given for incorrect ones. The decision-maker agent followed a similar reward structure, with rewards guiding the learning process toward accurate attack classification. The reward function was designed to provide higher feedback (value k) when an agent correctly classified its target attack and negative feedback for incorrect actions.

In this approach, cost-sensitive learning was used to assign rewards to L1 agents, where higher positive and negative feedback values k and $-k$ were provided for correct and incorrect predictions of the agent's attack class. This reward function encouraged the development of specialized agents for each type of attack, improving overall detection and classification accuracy despite class imbalances. Each agent focused on distinguishing its specific attack class from others, distributing the detection task among multiple agents. The reward policy for the decision-maker agent was simple:

$$R = \begin{cases} 1 \; if \; action = label \\ -1 \; if \; action \neq label \end{cases} \tag{1}$$

An improved weighted mean square error (WMSE) loss function was proposed for the DQN algorithm to handle class imbalance better. The loss function was designed to quantify the alteration among forecasted and target Q-values. The WMSE is defined as:

$$WMSE = \frac{1}{N}\sum_{i=1}^{N}\left(\left(Q(s_i, a_i) - q_{target}(s_i, a_i)\right).w_i\right)^2 \tag{2}$$

Where the target Q-value $q_{target}(s_i, a_i)$is computed as:

With each step concentrating on forecasting the attack class, the system's lack of state correlation led to the discount factor γ being near zero. Experiences in the replay memory were given weights; for L1 agents, these included samples pertaining to the agent's attack class, but for the decision-maker agent, minority classes received larger weights. This tactic reduced class disparity and enhanced the ability to identify various kinds of assault.

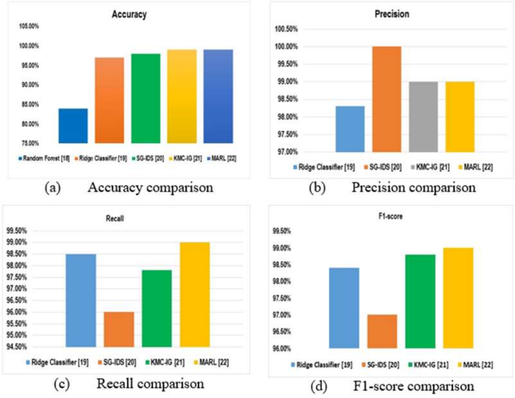
The effectiveness of the suggested IDS was evaluated using a comprehensive assessment of the CIC-IDS-2017 dataset. The evaluation began by describing the preprocessing steps applied to the dataset. Initially, records with infinite or missing values were removed to ensure stability during training. Z-score normalization was then utilized to scale the features, ensuring they exhibited a mean of zero and a standard deviation of one, a common technique for standardizing data. In the end, 80% of the dataset was set aside for training and 20% for testing, dividing it into two subsets: the training and testing sets. To balance the dataset, the number of normal traffic samples was reduced to match the number of malicious traffic samples.

The performance of the suggested MARL-based detection model was assessed by employing numerous performance metrics. The proposed IDS demonstrated exceptional detection capabilities, achieving a high accuracy of 99%. It also maintained a weighted recall of 99% and a low false positive rate of 0.0016%. The IDS effectively detected a wide range of attacks, including those with limited samples, demonstrating its ability to address the class imbalance issues in the CIC-IDS-2017 dataset. Additionally, it provided a precise classification of attacks and maintained high performance in identifying benign traffic. A comprehensive performance analysis compared the proposed IDS with existing model solutions that leveraged the CIC-IDS-2017 dataset. The results indicated that the proposed IDS exhibited exceptional capabilities in detecting all attacks, including minor classes, and accurately identifying benign traffic. This resulted in an impressively low false positive rate of 0.0016%, further highlighting the model's effectiveness in handling imbalanced class distributions while maintaining high detection rates.

This analysis highlighted the efficacy of the proposed multi-agent deep reinforcement learning architecture for ID. The modular design and improvements to the DQN algorithm enabled the system to adapt to evolving attack patterns and address the challenges of class imbalance. The results showed that the model provided superior detection rates and low FPR, making it a robust and scalable solution for network security in dynamic environments.

4. RESULT

In this section, the performance metrics are obtained from the papers analyzed in this analysis. The key performance indicators include accuracy, precision, recall, and F1-score, providing a comprehensive estimation of the effectiveness of existing methodologies. These metrics offer valuable insights into how well different ML techniques, including Random Forest, Ridge Classifier, Gaussian Naive Bayes, and MARL, have performed in detecting cyber-attacks. The analysis highlights the accuracy and robustness of each method, with some models achieving accuracy rates, underscoring their effectiveness in enhancing cybersecurity. Figure 2 shows the performance comparison for the analysed paper. In this graph, MARL demonstrates a significantly higher accuracy in detecting cyber-attacks than all other methods evaluated. This shows the efficiency of MARL in improving recognition capabilities within cybersecurity frameworks.



(a) Accuracy comparison

(b) Precision comparison

(c) Recall comparison

(d) F1-score comparison

Figure 2: Contrast of Performance metrics [30]

The ROC curve and AUC values for each attack type in the CIC-IDS-2017 dataset are depicted in Figure 3. The proposed IDS demonstrated excellent AUC results for most classes except for four out of fifteen. These four classes consisted of three web attacks, notably less contrasted to the other courses. Additionally, for the SSH Patator class, the reduced AUC value was attributed to the low data quality of this particular class within the CIC-IDS-2017 dataset. Consequently, the model encountered challenges in learning representative patterns, decreasing the AUC value.

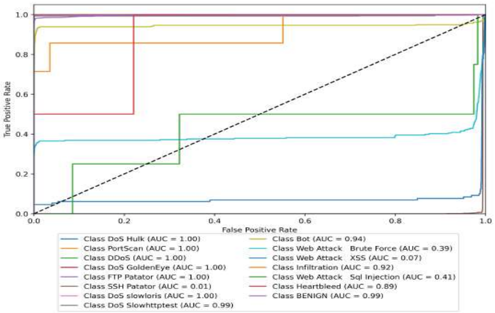


Figure 3: ROC curve for CIC-IDS 2017 dataset [30]

Furthermore, the false positive rates were also compared, and the MARL method demonstrated a lower false positive rate while effectively detecting all attacks, including minor classes. It also accurately identified benign traffic, achieving an impressively low false positive rate of 0.0016, notably better than the A-DQN network [31], which achieves 0.82%, as shown in Figure 4.

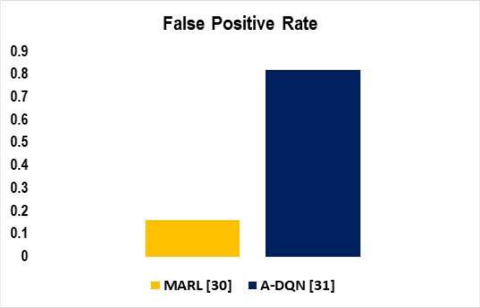


Figure 4 Comparison of False Positive Rate

The performance analysis of various machine learning techniques for cyber-attack detection clearly demonstrates that MARL outperforms other methods in accuracy, false positive rate, and overall detection capabilities. The ROC and AUC analysis further support its effectiveness in handling diverse attack types within datasets such as CIC-IDS-2017. Despite challenges with minor classes, MARL's adaptability and learning capabilities make it a highly effective solution for real-time cybersecurity frameworks. This reinforces MARL's potential as a robust and reliable approach for enhancing intrusion detection systems and addressing the complexities of evolving cyber threats.

5. DISCUSSION

In this analysis, we examined several ML techniques that have been applied to detect cyber-attacks, highlighting the increasing importance of ML in cybersecurity. ML has become vital for identifying patterns and anomalies in large datasets, enabling timely responses to emerging threats. Supervised, unsupervised, and reinforcement learning approaches are applied to expand the reliability and efficiency of cyber-attack detection. A security system leveraging the Ridge Classifier was developed in IoT environments to predict cyber-attacks. This study emphasized the significance of preprocessing and feature extraction, achieving an accuracy rate of 97%, highlighting the classifier's robustness in identifying potential threats and implementing real-time security measures. In the context of WSN, intrusion detection systems employing Gaussian Naive Bayes and SGD algorithms were explored. The study successfully reduced data dimensionality by utilising feature selection techniques such as PCA and SVD, resulting in an accuracy of 98%. This further demonstrated the model's efficiency in identifying CT in sensor-based environments. An intelligent hybrid model combining ML and AI techniques was also analyzed for its application in WSNs. By integrating feature reduction methods and K-Means Clustering, this model obtained an accuracy of 99% on the NSL-KDD dataset, underscoring the importance of data balancing and feature reduction in enhancing intrusion detection capabilities. This highlights the growing trend of hybrid cybersecurity approaches that leverage multiple algorithms' strengths to improve performance. A particularly noteworthy study introduced a MARL architecture to address challenges faced by traditional intrusion detection systems, such as class imbalance and the rapidly evolving nature of CT. By distributing the detection process across independent reinforcement learning agents, this architecture achieved a high accuracy of 99%, providing robust and adaptive detection across various attack types. This approach demonstrates the scalability and adaptability of MARL in addressing the complex and dynamic landscape of modern cyber threats. Despite the considerable progress made in applying ML for cyber-attack detection, the evolving nature of these threats necessitates ongoing adaptation and refinement of existing techniques. While many ML methods have proven effective across various fields, MARL has emerged as a particularly significant advancement due to its dynamic and decentralized approach to cybersecurity. Overall, these findings highlight the transformative potential of ML and AI in improving cybersecurity measures and underscore the need for continuous innovation to keep pace with the evolving threat landscape.

6. CONCLUSION

In conclusion, integrating ML approaches in cyber security demonstrates an outstanding advance in the fight over CT across various domains, including financial institutions, IoT networks, and wireless sensor networks. The studies reviewed demonstrate the effectiveness of various algorithms, such as RF, Ridge Classifier, Gaussian Naive Bayes, and MARL, in enhancing the accuracy and efficiency of cyber-attack detection. These approaches improve real-time threat identification and adapt to the dynamic nature of cyber threats, showcasing the potential for continuous innovation in security measures. As the landscape of CT evolves, adopting sophisticated techniques, particularly Multi-Agent Reinforcement Learning is essential for developing robust intrusion detection systems that can respond effectively to emerging challenges. The findings underscore the importance of ongoing research and development in ML applications, highlighting a collaborative approach to strengthening cybersecurity frameworks and safeguarding critical infrastructures. Future research in MARL should focus on optimizing agent cooperation and communication strategies to enhance detection capabilities against increasingly sophisticated cyber threats.

Solutions to Emerging Challenges

Several important challenges are outlined in this study that are detailed as follows:

- Dynamic Threat Adaptation: The rapid evolution of cyber threats makes it challenging to keep detection models updated, as traditional IDS struggle to identify new and sophisticated attack methods quickly.
- Scalability: Deploying IDS across complex and expansive IoT and WSN environments is difficult, as it requires solutions that can adapt to varied network structures and handle massive data volumes effectively.
- Handling Class Imbalance in Data: Many cyber-attack datasets contain an imbalance, with common attacks overrepresented and rare, potentially more harmful attacks underrepresented. This leads to reduced accuracy in detecting less frequent threats.

REFERENCES

[1] I. Naseer, "The efficacy of Deep Learning and Artificial Intelligence Framework in Enhancing Cybersecurity, Challenges and Future Prospects," *Innovative Computer Sciences Journal*, vol. 7, no. 1, 2021.

[2] M. A. I. Mallick and R. Nath, "Navigating the Cybersecurity Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments," *World Scientific News*, vol. 190, no. 1, pp. 1–69, 2024.

[3] V. Demertzi, S. Demertzis, and K. Demertzis, "An overview of cyber threats, attacks and countermeasures on the primary domains of smart cities," *Applied Sciences*, vol. 13, no. 2, p. 790, 2023.

[4] P. Wanda and H. J. Jie, "A survey of intrusion detection system," *International Journal of Informatics and Computation*, vol. 1, no. 1, pp. 1–10, 2020.

[5] F. Jemili, R. Meddeb, and O. Korbaa, "Intrusion detection based on ensemble learning for big data classification," *Cluster Computing*, vol. 27, no. 3, pp. 3771–3798, 2024.

[6] M. Sarhan, S. Layeghy, and M. Portmann, "Feature analysis for machine learning-based IoT intrusion detection," *arXiv preprint arXiv:2108.12732*, 2021.

[7] T. Ferrão, F. Manene, and A. A. Ajibesin, "Multi-Attack Intrusion Detection System for Software-Defined Internet of Things Network," *Computers, Materials & Continua*, vol. 75, no. 3, 2023.

[8] E. Oluwawemimo, "The Role of Artificial Intelligence in Incident Response for Digital Domain SMEs," 2024.

[9] S. Muneer, U. Farooq, A. Athar, M. Ahsan Raza, T. M. Ghazal, and S. Sakib, "A Critical Review of Artificial Intelligence Based Approaches in Intrusion Detection: A Comprehensive Analysis," *Journal of Engineering*, vol. 2024, no. 1, 2024.

[10] O. C. Obi, O. V. Akagha, S. O. Dawodu, A. C. Anyanwu, S. Onwusinkwue, and I. A. I. Ahmad, "Comprehensive review on cybersecurity: modern threats and advanced defense strategies," *Computer Science & IT Research Journal*, vol. 5, no. 2, pp. 293–310, 2024.

[11] A. Wong, T. Bäck, A. V. Kononova, and A. Plaat, "Deep multiagent reinforcement learning: Challenges and directions," *Artificial Intelligence Review*, vol. 56, no. 6, pp. 5023–5056, 2023.

[12] M. N. Naby Ndiaye, H. El Bergou, and H. El Hammouti, "Age-of-Information in UAV-assisted Networks: a Decentralized Multi-Agent Optimization," *arXiv e-prints, arXiv-2312*, 2023.

[13] Z. Ning and L. Xie, "A survey on multi-agent reinforcement learning and its application," *Journal of Automation and Intelligence*, 2024.

[14] F. Louati, F. Barika Ktata, and I. Amous, "An intelligent security system using enhanced anomaly-based detection scheme," *The Computer Journal*, 2024, doi:10.1093/comjnl/bxae008.

[15] Y. L. Khaleel, M. A. Habeeb, A. S. Albahri, T. Al-Quraishi, O. S. Albahri, and A. H. Alamoodi, "Network and cybersecurity applications of defense in adversarial attacks: A state-of-the-art using machine learning and deep learning methods," *Journal of Intelligent Systems*, vol. 33, no. 1, p. 20240153, 2024.

[16] A. Alshamrani and A. Alshahrani, "Adaptive Cyber Defense Technique Based on Multiagent Reinforcement Learning Strategies," *Intelligent Automation & Soft Computing*, vol. 36, no. 3, 2023.

[17] F. Rossi, S. Bandyopadhyay, M. T. Wolf, and M. Pavone, "Multi-agent algorithms for collective behavior: A structural and

application-focused atlas," *arXiv preprint arXiv:2103.11067*, 2021.

[18] E. C. Pinto Neto, S. Sadeghi, X. Zhang, and S. Dadkhah, "Federated reinforcement learning in IoT: applications, opportunities and open challenges," *Applied Sciences*, vol. 13, no. 11, p. 6497, 2023.

[19] Z. Pelletier and M. Abualkibash, "Evaluating the CIC IDS-2017 dataset using machine learning methods and creating multiple predictive models in the statistical computing language R," *Science*, vol. 5, no. 2, pp. 187–191, 2020.

[20] R. Golchha, A. Joshi, and G. P. Gupta, "Voting-based ensemble learning approach for cyber-attacks detection in Industrial Internet of Things," *Procedia Computer Science*, vol. 218, pp. 1752–1759, 2023.

[21] M. N. Alatawi, N. Alsubaie, H. U. Khan, T. Sadad, H. S. Alwageed, S. Ali, and I. Zada, "Research Article Cyber Security against Intrusion Detection Using Ensemble-Based Approaches," 2023.

[22] B. Rababah and S. Srivastava, "Hybrid model for intrusion detection systems," *arXiv preprint arXiv:2003.08585*, 2020.

[23] B. Uzun and S. Ballı, "A novel method for intrusion detection in computer networks by identifying multivariate outliers and ReliefF feature selection," *Neural Computing and Applications*, vol. 34, no. 20, pp. 17647–17662, 2022.

[24] E. Y. Güven, S. Gülgün, C. Manav, B. Bakır, and G. Z. G. Aydın, "Multiple classification of cyber attacks using machine learning," *Electrica*, vol. 22, no. 2, pp. 313–320, 2022.

[25] S. Ouiazzane, M. Addou, and F. Barramou, "A Suricata and Machine Learning Based Hybrid Network Intrusion Detection System," in *Advances in Information, Communication and Cybersecurity: Proceedings of ICI2C'21*, Springer International Publishing, pp. 474–485, 2022.

[26] M. R. Labu and M. F. Ahammed, "Next-Generation cyber threat detection and mitigation strategies: a focus on artificial intelligence and machine learning," *Journal of Computer Science and Technology Studies*, vol. 6, no. 1, pp. 179–188, 2024.

[27] A. Alomiri, S. Mishra, and M. AlShehri, "Machine learning-based security mechanism to detect and prevent cyber-attack in IoT networks," *International Journal of Computing and Digital Systems*, vol. 16, no. 1, pp. 645–659, 2024.

[28] H. M. Saleh, H. Marouane, and A. Fakhfakh, "Stochastic Gradient Descent Intrusions Detection for Wireless Sensor Network Attack Detection System Using Machine Learning," 2024.

[29] M. H. Behiry and M. Aly, "Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods," *Journal of Big Data*, vol. 11, no. 1, p. 16, 2024.

[30] A. Tellache, A. Mokhtari, A. Amara Korba, and Y. Ghamri-Doudane, "Multi-agent Reinforcement Learning-based Network Intrusion Detection System," *arXiv e-prints, arXiv-2407*, 2024.

[31] K. Sethi, Y. V. Madhav, R. Kumar, and P. Bera, "Attention based multi-agent intrusion detection systems using reinforcement learning," *Journal of Information Security and Applications*, vol. 61, p. 102923, 2021.