Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.064728

ARTICLE

Unveiling CyberFortis: A Unified Security Framework for IIoT-SCADA Systems with SiamDQN-AE FusionNet and PopHydra Optimizer

Kuncham Sreenivasa Rao[1], **Rajitha Kotoju**[2], **B. Ramana Reddy**[3], **Taher Al-Shehari**[4], **Nasser A. Alsadhan**[5], **Subhav Singh**[6,7,8] **and Shitharth Selvarajan**[9,10,11,*]

[1]Department of Computer Science and Engineering, Faculty of Science and Technology (ICFAITech), ICFAI Foundation for Higher Education, Hyderabad, 501203, India
[2]Department of Computer Science and Engineering, Mahatma Gandhi Institute of Technology, Hyderabad, 500075, India
[3]Department of CSE, Chaitanya Bharathi Institute of Technology, Hyderabad, 500075, India
[4]Computer Skills, Department of Self-Development Skill, Common First Year Deanship, King Saud University, Riyadh, 11362, Saudi Arabia
[5]Computer Science Department, College of Computer and Information Sciences, King Saud University, Riyadh, 12372, Saudi Arabia
[6]Chitkara Centre for Research and Development, Chitkara University, Solan, 174103, India
[7]Division of Research & Innovation, Uttaranchal University, Dehradun, 248007, India
[8]Division of Research and Development, Lovely Professional University, Phagwara, 144411, India
[9]School of Built Environment, Engineering and Computing, Leeds Beckett University, Leeds, LS6 3HF, UK
[10]Department of Computer Science and Engineering, Chennai Institute of Technology, Chennai, 600069, India
[11]Centre for Research Impact & Outcome, Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, 140401, India

*Corresponding Author: Shitharth Selvarajan. Email: s.selvarajan@leedsbeckett.ac.uk

Received: 22 February 2025; Accepted: 21 July 2025; Published: 29 August 2025

ABSTRACT: Protecting Supervisory Control and Data Acquisition-Industrial Internet of Things (SCADA-IIoT) systems against intruders has become essential since industrial control systems now oversee critical infrastructure, and cyber attackers more frequently target these systems. Due to their connection of physical assets with digital networks, SCADA-IIoT systems face substantial risks from multiple attack types, including Distributed Denial of Service (DDoS), spoofing, and more advanced intrusion methods. Previous research in this field faces challenges due to insufficient solutions, as current intrusion detection systems lack the necessary accuracy, scalability, and adaptability needed for IIoT environments. This paper introduces CyberFortis, a novel cybersecurity framework aimed at detecting and preventing cyber threats in SCADA-IIoT systems. CyberFortis presents two key innovations: Firstly, Siamese Double Deep Q-Network with Autoencoders (Siamdqn-AE) FusionNet, which enhances intrusion detection by combining deep Q-Networks with autoencoders for improved attack detection and feature extraction; and secondly, the PopHydra Optimiser, an innovative solution to compute reinforcement learning discount factors for better model performance and convergence. This method combines Siamese deep Q-Networks with autoencoders to create a system that can detect different types of attacks more effectively and adapt to new challenges. CyberFortis is better than current top attack detection systems, showing higher scores in important areas like accuracy, precision, recall, and F1-score, based on data from CICIoT 2023, UNSW-NB 15, and WUSTL-IIoT datasets. Results from the proposed framework show a 97. 5% accuracy rate, indicating its potential as an effective solution for SCADA-IIoT cybersecurity against emerging threats. The research confirms that the proposed security and resilience methods are successful in protecting vital industrial control systems within their operational environments.

Copyright © 2025 The Authors. Published by Tech Science Press.
This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

KEYWORDS: Industrial Internet of Things (IIoT); SCADA systems; security; intrusion detection system (IDS); optimization; deep learning

1 Introduction

Industrial Internet of Things (IIoT) devices are very acute in the management of urban-related critical infrastructure, including smart grids, water distribution networks, and transportation systems [1,2]. Systems such as Supervisory Control and Data Acquisition (SCADA) play a crucial role in monitoring and controlling these infrastructures. Again, in IIoT devices used in the control and monitoring of utilities like water and electricity supply, any disturbance in the functioning of these IIoT devices, particularly cyber-attacks on these IIoT devices may cause damages that are damaging to the very infrastructure of a modern urban environment. SCADA systems, being at the core of most critical functions in these sectors, leave them highly vulnerable to attacks that can cause troubles, starting from service outages to more disastrous consequences, including environmental hazards or threats to public safety. This makes SCADA systems even more critical in IIoT due to their much larger geographical scale of operation than most other industrial control systems [3]. However, this widespread coverage, which benefits the administration of large-scale infrastructures, also opens the way for other problems related to communication. Because most SCADA systems communicate over extensive distances via telephony or third-party networks, data transmission is plagued by lower speeds, low frequency, and poor quality in most cases. Typically, the communications infrastructure lacks speed and reliability, making it difficult to provide real-time or continuous updates to SCADA systems [4]. Typically, they adhere to an event-driven model, transmitting data only upon detecting a significant change in any monitored value or condition.

For instance, if a sensor detects a sudden rise in pressure inside a water pipeline, such an event will be logged by the SCADA system, which will then raise an alarm with the operators for action. Moreover, since SCADA systems often use third-party or public communication networks for their operation, the security of these networks becomes a major concern. SCADA and IIoT systems could increase the possibility of cyber-attacks [5,6]; malicious actors are able to compromise the security integrity of such a system through those vulnerabilities from IIoT communication channels. An increased exposure through the requirement that these control systems rely more heavily on the availability of exterior network communication resources results in an increased attack surface to the traditional set of challenges faced by security for SCADA. Thus, knowledge of vulnerabilities and operational characteristics of IIoT-SCADA systems is very instrumental in improving the security and resilience of these infrastructures. The management of long-distance communications, besides being inherently difficult due to the complexity of IIoT networks, must protect the SCADA systems involved from cyberattacks. In a nutshell, IIoT is the adaptation of Internet of Things technology that is made available for industrial applications. The IIoT uses connectivity and data exchange characteristics of IoT devices to enhance the effectiveness and efficiency of services provided by industrial systems, including their reliability. In this aspect, many IIoT devices [7] and sensors have been inducted into many industrial procedures, including manufacturing plants, energy grids, transportation, and supply chain management. These devices collect and transmit reams of real-time data, enabling industries to optimize operations, anticipate maintenance needs, and raise overall system performance. With the rapid deployment of IIoT networks in various industrial sectors, a major challenge will be exposing these networks to various security vulnerabilities. The larger the number of IIoT devices that proliferate, the more they are deployed in isolated, sometimes legacy networks, and the more security breaches will increase.

To mitigate these risks, an IDS becomes an important component in securing the IIoT environment. IDS is designed for monitoring activities taking place within the network and pointing out any such behaviour that reflects anomalies, whether from malicious actors or cyberattacks. The IDS has a single mission: to detect suspicious activity and generate the necessary alert to system administrators, who can then take proactive actions to avoid or mitigate security breaches [8]. IIoT systems are very different from traditional information technology (IT) networks, and their configuration poses several challenges that make the deployment of conventional IDS mechanisms in IIoT environments very challenging. One of the key challenges is the very nature of IIoT devices, which usually have constraints related to resources. The devices in question are usually embedded systems with very small processing power, memory, and storage capacity. The volume of data out of IIoT systems, therefore, presents a challenge for IDS systems since processing and analyzing such huge data in real-time could also be computationally overwhelming for thin resources of single devices. IIoT systems also have a very large number of data privacy concerns. These privacy issues make it critical that security solutions, including IDS systems, are designed in such a manner that the confidentiality of the data being transmitted must be ensured with the integrity of the network [9]. Unlike homogeneous IT systems, where the devices usually follow similar protocols and standards, the IIoT networks are highly fragmented, which makes it increasingly difficult for a traditional IDS to guarantee uniform coverage and threat detection capabilities over the whole network. Considering the above-mentioned challenges, it would not only be very challenging from a technical point of view but also inefficient to deploy a traditional IDS in IIoT. Equally, the IDS solutions have to be flexible enough to adjust to the diversities in communication protocols and security needs of the IIoT networks.

With the IIoT-SCADA systems under increasing frequency and sophistication of cyber-attacks, industrial infrastructure is at a critical juncture where strong security mechanisms are in place to ensure efficient intrusion detection and mitigation. The traditional IDS solutions face several challenges due to the unique features of the IIoT-SCADA environment, such as limited resources, data privacy concerns, and different types of networks [10,11]. For that purpose, a deep-learning-based IDS shall be responded to in such a manner that the accuracy of the threat detection mechanism is enhanced and can adapt over time to evolving patterns of attack and efficiently operate within IIoT-SCADA frameworks. The industrial control system should incorporate real-time anomaly detection features using advanced neural network techniques, which would reduce the likelihood of cyber threats and consequently enhance the overall security and reliability of these systems.

The paper organizes itself to provide a thorough examination of the security of IIoT-SCADA systems through the lens of a deep learning-based IDS. Section 2 performs the literature review of the already existing security models proposed for protection in the IIoT-SCADA environment. Section 3 describes the deep learning-based IDS that has been proposed in detail with its architecture, methodologies, and how it will address the challenges in IIoT-SCADA security. Section 4 gives the performance evaluation of the proposed model, whose comparative findings against traditional security mechanisms are conducted to prove its effectiveness. Finally, Section 5 summarizes the key points of the paper, emphasizing the impact of the proposed approach and outlining future research directions for enhancing IIoT-SCADA security.

2 Literature Review

Research into protecting Industrial Internet of Things (IIoT)-SCADA systems has become essential because attacks against industrial control networks continue to increase. The resilience of IIoT-SCADA environments receives improvements from different security models that use traditional signature-based intrusion detection systems (IDS) [12], anomaly detection and hybrid detection approaches. Current solutions struggle with scalability problems as well as resource limitations during their operation and require modification for new attack approaches to work. The section analyzes recent security models designed for IIoT-SCADA systems through operational analysis of their approaches while showing their weaknesses.

Srinivasan and Senthilkumar [13] stated that IIoT network security gets enhanced through a joint solution that combines Convolutional Neural Networks (CNNs) for pattern detection with a blockchain-reinforced Reinforcement Learning (RL) system for automated threat defence. CNNs show proven success in intrusion defence through abnormal traffic detection, which makes them appropriate for IIoT applications because network traffic data operates in high dimensions and possesses complexity. The use of blockchain improves security infrastructure through complete data protection and protected network connections that benefit distributed IIoT platforms. The main innovation of this study originates from its reinforcement learning system that evolves automatically to address changing threats, thus providing immediate defence choices and proactive protection strategies. Strengthening the study's contribution requires more detail about the performance benefits and computation speed, together with the deployment practicality of the hybrid technique. Benka et al. [14] propose a multi-model approach for anomaly detection that captures both spatial and temporal patterns in network traffic. A major strength of the research lies in creating a dedicated dataset that includes ICS communication patterns under normal operation and manipulated datasets, with focused attention on the Transmission Control Protocol/Internet Protocol (TCP/IP) traffic. It would be of extreme importance to simulate lateral attacks over this data; this will emulate actual cyber threats; thus, the machine learning (ML) model designed with this data set will be resilient. A further discussion about the scalability and feasibility of deploying these models in real ICS environments definitely increases the practical relevance of the research.

Zeng et al. [15] introduce EvoAAE, a new automated adversarial deep learning-based unsupervised anomaly detection method, for the security of IIoT networks. In this way, the proposed approach uses an adversarial variational autoencoder enriched by a generative adversarial network responsible for generating adversarially multivariate time series with sophisticated anomaly detection in complex IIoT environments. The key improvement is combining Particle Swarm Optimization (PSO) with a smart way to encode data, which helps adjust the hyperparameters and neural structures. The proposed method uses a special type of autoencoder, enhanced by a generative adversarial network, to create complex time series data that helps detect unusual patterns in complicated IIoT settings. The results would help further in comparing EvoAAE scalability in large-scale IIoT networks and hence show its effectiveness and the practicality of its deployment. Yalcin et al. [10] developed an AI-based Intrusion Detection System with high accuracy for the security of SCADA systems, focusing on the identification of cyberattacks that could compromise the integrity of these critical infrastructures. This paper utilizes various Artificial Intelligence (AI) techniques to construct AI models with different parameters, such as K-nearest neighbour (KNN), quadratic discriminant analysis (QDA), adaptive boosting (AdaBoost), gradient boosting (GB), and random forest (RF), in order to address the diverse nature of potential cyber threats to SCADA systems. The authors experiment on two different SCADA datasets to improve detection performance under different attack scenarios. Their results would, however, be more promising in the enhancement of SCADA security, providing more details on comparative performance between the models in terms of detection accuracy, false-positive rates, and computational efficiency. Bansal and Singhrova [16] discussed the development of IDS as a solution for meeting challenges in security and privacy associated with detecting a wide range of attacks in IoT/IIoT. They point out the diversity of IDS methodologies used in such systems for identifying intrusions in IoT/IIoT networks, but the detection capabilities need further enhancement. The approach is very useful for highlighting the gaps in the current IDS technologies and putting much emphasis on areas where innovations are needed: improving adaptability, scalability, and real-time performance of the detection systems.

Sangoleye et al. [17] provide a novel study on the application of different Deep Reinforcement Learning models, such as Deep Q-Network (DQN), Double Deep Q-Network (DDQN), Dueling Double Deep Q-Network (D3QN), REINFORCE, Advantage Actor-Critic (A2C), and Proximal Policy Optimization

(PPO), to network intrusion detection in Industrial Control Systems (ICS). The authors recognize that testing in a real ICS setting is challenging, so they use labelled pre-recorded intrusion datasets to evaluate how well the models perform in a controlled environment. Several essential research gaps emerge from the literature review that evaluate intrusion detection systems (IDS) for the Industrial Internet of Things (IIoT) and Industrial Control Systems (ICS) regarding advanced machine learning and deep learning model applications. Traditional IDS approaches utilize signature-based along with anomaly-based detection techniques, although they prove inadequate when detecting behaviours in IIoT networks because these environments present dynamic characteristics combined with heterogeneous systems connected with limited resources. The present security techniques fail to achieve sustainable growth together with real-time response capabilities and system adaptation for emerging threats when securing IIoT networks. Deep reinforcement learning (DRL) models and their related reinforcement learning (RL) models are becoming popular for making decisions about threat management, but they are hard to use in ICS and IIoT environments because they are complicated to calculate and test in real-world systems. The application of blockchain for IIoT security remains a developing field and researchers have not explored its potential integration with deep learning-based IDS for providing complete security solutions. IDS solutions need to be improved to be more adaptable and able to grow because these technologies must overcome current limitations in environments with limited resources while also meeting real-time needs and handling complex data.

3 Proposed Methodology

The proposed work presents a new method for securing the IIoT-SCADA systems against some of the new kinds of cyber threats emerging from the IoT. This research focuses on a new type of cybersecurity framework, called CyberFortis, that is robust, adaptive, and, most importantly, designed to significantly improve real-time intrusion detection and prevention in IIoT-SCADA systems. But CyberFortis is a model by virtue of which an Intelligent Intrusion Detection System (IIDS) is being developed, and this system, quite unlike any seen before, promises to fill some of those aforementioned security holes. The methods put forth in the CyberFortis model use the latest artificial intelligence and optimization techniques. One of the most important aspects of this work is the use of a feedback loop guided by reinforcement learning principles. Indeed, at the level of artificial intelligence, the CyberFortis work is significant because it makes good use of several crucial components and seemingly blends them together smoothly. Another major thing that the work achieves (or one that it claims to achieve) is that it manages to blend these various artificial intelligence components together and comes out with a piece of work that has very much the look and feel of a smoothly integrated system. Initially, this model encompasses an adaptive and direct security response to threats for IIoT-SCADA systems. These systems are implemented more often in industrial settings, which makes the security and reliability of the systems all the more critical. The IIoT offers an increasing number of opportunities for infiltration; all industrial entities are subject to the risk associated with being digitally connected.

This paper aims to design SiamDQN-AE FusionNet, which will tackle the difficulties associated with intrusion detection in IIoT-SCADA systems with complex multilayer data structures, massive networks, and real-time requirements. As shown in Fig. 1, templates from the Autoencoders and the Double Deep Q Network (DDQN) are used to modify intrusion detection systems using novel techniques capable of learning spatiotemporal features over the network flows. Siamese networks (SNN), which utilize a pair of neural networks in a single overarching neural network architecture, are adept at the differentiation between normal and intrusion behavioural patterns in an IIoT ecosystem. With the SNN architecture, it is possible for the model to detect minute discrepancies in data such that even traditional IDS systems would find it challenging to perform. In addition, DDQN allows for handling a large action space while simultaneously learning the best-known detection methods for different IVs using reinforcement learning for improved distribution adaptability. Furthermore, the Autoencoder part of the model makes the system capable of feature extraction in the scope of unsupervised learning, thereby facilitating the model's ability to solve problems with sparsely labelled data, which is a normal problem in IIoT systems.

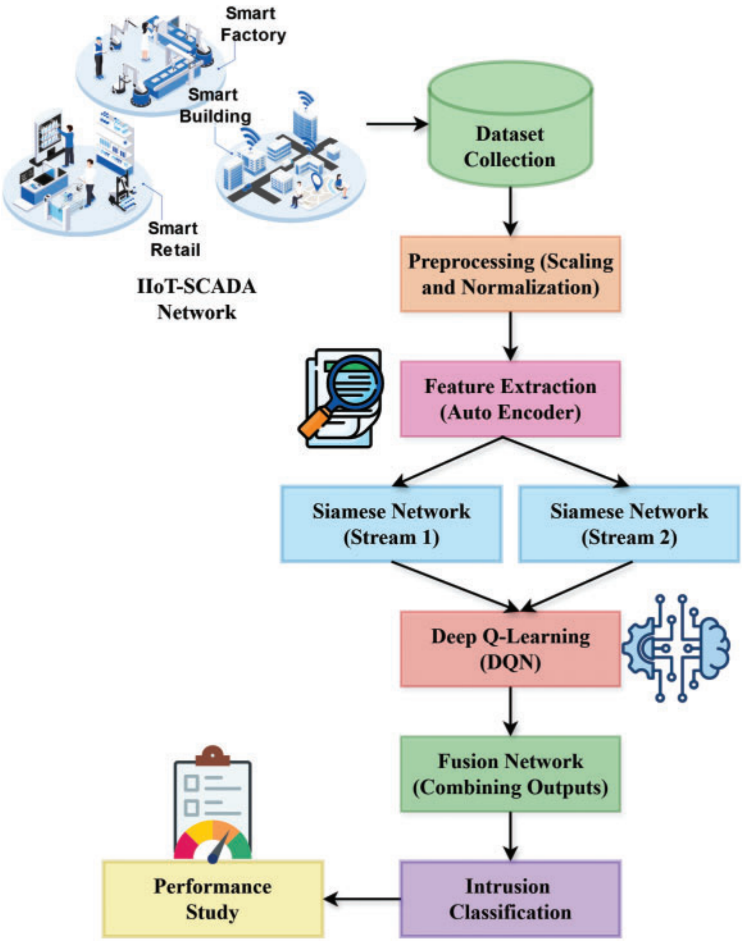
Smart Factory
Smart Building
Smart Retail
IIoT-SCADA Network
Dataset Collection
Preprocessing (Scaling and Normalization)
Feature Extraction (Auto Encoder)
Siamese Network (Stream 1)
Siamese Network (Stream 2)
Deep Q-Learning (DQN)
Fusion Network (Combining Outputs)
Intrusion Classification
Performance Study

Figure 1: Overview of the proposed work

The discount factor computation has been enhanced by the incorporation of the PopHydra Optimizer in the CyberFortis model. It optimizes decision-making at the level of the Intrusion Detection System. Within SiamDQN-AE FusionNet, reinforcement learning algorithms are used as a component, and the discount factor is one of the most vital parameters that determines how rewards in the future are valued as compared to the rewards in the present. To crunch this parameter, a hybrid technique called PopHydra Optimizer, which edges out in the combination of Poplar Optimization and Waterwheel Plant Algorithm, is introduced.

3.1 SiamDQN-AE FusionNet for Intrusion Detection in IIoT-SCADA Systems

SiamDQN-AE FusionNet is one of the first mixed models introduced in this paper, which combines Siamese Networks, Double Deep Q-Networks, and Autoencoders to tackle complex security issues in IIoT environments, such as SCADA systems. The technique aims to merge the benefits of each part to improve intrusion detection, where the Siamese network helps learn features and spot unusual activities, and DDQN offers smart decision-making and better classification. At the same time, Autoencoders detect subtle deviations from normal operational patterns that help identify possible cyber-attacks. The learning models are combined into the SiamDQN-AE FusionNet framework so that the system can better recognize both familiar and new types of attacks with greater accuracy and fewer false alarms. To our knowledge, this synergic integration of those cutting-edge models by the SiamDQN-AE FusionNet for IIoT-SCADA intrusion detection has not been much explored in state-of-the-art IDS. Each of them brings a unique benefit: the Siamese network is good at measuring similarity between input samples and, thus, good at spotting pairs of data that are anomalous, not conforming to normal behaviour in the system. Finally, the autoencoder focuses on reconstructing data based on learned patterns and flagging deviations as anomalies. Such a combination of models gives an end-to-end solution capable of detecting not only suspicious network traffic but also learning from the environment in real-time to adapt to new unseen attacks.

This technique is novel to all the other existing models, as it merges unsupervised learning through the autoencoder with reinforcement learning using DDQN and supervised feature learning via the Siamese network in an attempt to construct a powerful, multi-layered defence against a broad range of attack types. The SiamDQN-AE FusionNet is much more powerful, as it fuses three important paradigms to increase the detection capabilities and adaptability of the system, as opposed to the traditional IDS models that mostly depend on rule-based approaches or single-method machine-learning models. Most of the IDS solutions available in the market either focus on known attack detection or are reactive. The learning models are combined into the SiamDQN-AE FusionNet framework so that the system can better recognize both familiar and new types of attacks with greater accuracy and fewer false alarms. First, IIoT systems are usually overwhelmed by a large amount of data with normal and malicious behaviours interwoven; this technique is effective at distinguishing subtle anomalies from legitimate operations through deep learning and unsupervised methods. Second, the DDQN component is suitable for an environment where decisions have to be made based on evolving patterns and real-time data, a common feature of IIoT-SCADA systems. It becomes adaptive and strong in the identification of new attack vectors since it can adapt the detection strategy to current network traffic and attack behaviours. Initially, the detection mechanism computes the Siamese distance function using the following mathematical model:

$$\delta\left(h_1, h_2\right) = \left\| f\left(h_1\right) - f\left(h_2\right) \right\|_2 \tag{1}$$

where $f(h)$ indicates the feature extraction function of the Siamese network, and $||.||$ is the Euclidean distance function. As a consequence of this, the contrastive loss function is computed with the following equation:

$$\mathcal{L} = \frac{1}{2} x \times \delta\left(h_1, h_2\right)^2 + (1 - x) \times \max(0, \beta - \delta\left(h_1, h_2\right))^2 \tag{2}$$

where $x \in \{0, 1\}$ represents the pair and β denotes the margin. Consequently, the Siamese network objective function is estimated for spotting intrusions according to the following model:

$$\mathcal{L}_{Sia} = \sum_{i=1}^{N} \mathbb{L}_i(x_i, \delta\left(h_1\right), \delta(h_2)) \tag{3}$$

where N indicates the total number of samples, and $\mathbb{L}_i$ represents the loss between the predicted and actual labels. Furthermore, the cosine similarity function is also estimated with L2 normalization based on the following equation:

$$\mathcal{S}\left(h_1, h_2\right) = \frac{f\left(h_1\right) \times f(h_2)}{\left\| f\left(h_1\right) \right\|_2 \left\| f\left(h_2\right) \right\|_2} \tag{4}$$

where $\|\square\|$ is the L2 normalization function. Then, the Siamese network's output is obtained, which is in the following form:

$$\hat{p} = \varphi(\varpi^{K} f\,(h_1, h_2) + \mathfrak{B}) \tag{5}$$

where ϖ and $\mathfrak{B}$ are the learnable parameters, and φ represents the sigmoid activation function. In addition to that, the Double DQN model is integrated with the Siamese network, in which the Q-learning update rule is carried out at first according to the following equation:

$$\mathcal{Q}^{\pi}\,(\mathscr{s}_k, \mathscr{a}_k) \leftarrow \mathcal{Q}^{\pi}\,(\mathscr{s}_k, \mathscr{a}_k) + \tau \times \mathscr{r}_k + \mathfrak{F} \max_{\mathscr{a}'} \mathcal{Q}\,(\mathscr{s}_{k+1}, \mathscr{a}') - \mathcal{Q}(\mathscr{s}_k, \mathscr{a}_k) \tag{6}$$

$$\mathcal{Q}^{\pi}\,(\mathscr{s}_k, \mathscr{a}_k) \leftarrow \mathcal{Q}^{\pi}\,(\mathscr{s}_k, \mathscr{a}_k) + \tau \times \mathscr{r}_k + \mathfrak{F}\mathcal{Q}\left(\mathscr{s}_{k+1}, \arg\max_{\mathscr{a}'} \mathcal{Q}(\mathscr{s}_{k+1}, \mathscr{a}')\right) - \mathcal{Q}(\mathscr{s}_k, \mathscr{a}_k) \tag{7}$$

where $\mathcal{Q}(\mathscr{s}_k, \mathscr{a}_k)$ indicates the action-value function, τ represents the learning rate, and $\mathfrak{F}$ is the discount factor. Then, the advantage function is computed for the DDQN model using the following equation:

$$\mathcal{A}\,(\mathscr{s}_k, \mathscr{a}_k) = \mathcal{Q}\,(\mathscr{s}_k, \mathscr{a}_k) - \mathfrak{v}(\mathscr{s}_k) \tag{8}$$

where $\mathfrak{v}(\mathscr{s}_k)$ is the state-value function, and $\mathcal{A}\,(\mathscr{s}_k, \mathscr{a}_k)$ denotes the advantage of taking action for state. Here, the Bellman equation is also applied for computing the Q-value as shown below:

$$\mathcal{Q}^{\pi}\,(\mathscr{s}, \mathscr{a}) = \mathcal{E}\mathscr{r} + \mathfrak{F} \max_{\mathscr{a}'} \mathcal{Q}\,(\mathscr{s}', \mathscr{a}') \tag{9}$$

Furthermore, the target network rule is updated with respect to the update rate, as shown in the following equation:

$$\eta' \leftarrow \wp\eta + (1 - \wp)\eta' \tag{10}$$

where η and η' are the Q-network and target network parameters, respectively, and $\wp$ represents the update rate. Furthermore, the autoencoder loss function is updated based on the following model:

$$\mathbb{L}_{AE} = \frac{1}{N} \sum_{i=1}^{N} \left\| h_i - \hat{h}_i \right\|^2 \tag{11}$$

where N is the total number of samples, h_i and $\hat{h}_i$ are the input and reconstruction parameters. Then, the encoder function is calculated with respect to the encoder weight matrix and bias value, as shown in the following equation:

$$\mathscr{h} = \phi(\varpi_e h + \mathfrak{B}) \tag{12}$$

where ϕ is the activation function, ϖ_e denotes the encoder weight matrix, and $\mathfrak{B}$ represents the bias term. Similarly, the decoder function is also estimated using the following equation:

$$\hat{h} = \phi(\varpi_d h + \mathfrak{B}) \tag{13}$$

where ϖ_d is the decoding weight matrix, for the fusion net, the integrated loss function is estimated according to the following model:

$$\mathbb{L}_{fusion} = \xi_1 \mathbb{L}_{sia} + \xi_2 \mathbb{L}_{DQN} + \xi_3 \mathbb{L}_{AE} \tag{14}$$

where ξ_1, ξ_2, ξ_3 are the weight coefficients. Furthermore, the action selection is performed with respect to the Q-values predicted by the DDQN model, which is mathematically expressed as follows:

$$\mathcal{a}_k = \arg\max_{a'} \mathcal{Q}\left(\mathcal{s}_k, \mathcal{a}'\right) \tag{15}$$

Then, the intrusion score is estimated with the fusion net model, and its output is in the following form:

$$\hat{p} = \phi\left(\varpi_{\mathfrak{f}}^{K} \times \mathfrak{f}_{fusion}\left(h_1, h_2\right) + \mathfrak{B}_{\mathfrak{f}}\right) \tag{16}$$

where $\mathfrak{f}_{fusion}\left(h_1 \text{ and } h_2\right)$ indicate the fused features of Siamese, DDQN and AE networks, the corresponding reward function for the fusion net is estimated based on the following model:

$$\mathcal{R}_k = -\mathbb{L}_{fusion}(h_k, \hat{h}_k) \tag{17}$$

where $\mathcal{R}_k$ represents the reward function.

Algorithm 1 outlines the steps of the proposed SiamDQN-AE FusionNet model, which integrates a Siamese architecture with DQN and AE models for robust feature fusion and decision-making.

Algorithm 1: Proposed SiamDQN-AE FusionNet model

```
Step 1: The given input dataset, $H = \{h_1, h_2, \ldots, h_n\}$ is initialized, which comprises both normal and anomalous traffic features;
Step 2: To ensure stabilized model training, the data normalization and scaling are performed;
Step 3: Apply the Siamese network model for feature learning;
    $\mathcal{L} = \frac{1}{2} x \times \delta\left(h_1, h_2\right)^2 + (1 - x) \times \max(0, \beta - \delta\left(h_1, h_2\right))^2$
Step 4: Then, the autoencoder training is applied for anomaly detection $\hat{h} = AE(h)$;
Step 5: Compute reconstruction error $\mathcal{L} = \left\|h - \hat{h}\right\|_2^2$;
Step 6: Apply double DQN for making effective decisions;
Initialize network $\mathcal{Q}(\mathcal{s}_k, \mathcal{a}_k)$ with action and state;
Compute $\mathcal{a}_k = \arg\max_a \mathcal{Q}(\mathcal{s}_k, \mathcal{a})$;
In order to reduce the overestimation bias, the target network update is performed;
Similarly, the double DQN state is also updated $\mathcal{Q}(\mathcal{s}_k, \mathcal{a}_k)$;
Step 7: Fuse the outputs of Siamese, DQN and AE networks;
Compute the similarity score $\mathfrak{f}_{sia}(h_1, h_2)$;
Compute reconstruction error $\mathbb{L}_{AE}$;
Obtain the output of DDQN;
Obtain the final output of the fusion network;
Step 8: Compute the loss function $\mathbb{L}_{fusion}$.
```

3.2 PopHydra Optimizer for Discount Factor Computation

PopHydra Optimizer for Discount Factor Calculation is a new approach with the potential to improve the accuracy and efficiency of discount factor calculation in decision-making models, especially in application fields such as IDS for IIoT-SCADA systems. The optimization of decision-making parameters, specifically the discount factor, is the core idea of this approach and serves as an important building block for reinforcement learning models in Intrusion Detection Systems (IDS). The discount factor determines the value of future rewards to be obtained against immediate rewards in learning models and thus has a very important impact on the performance of long-term predictive accuracy and decision-making in cybersecurity. In IIoT-SCADA systems, a sophisticated cyberattack, an optimal discount factor can improve the detection rate and response rate of an IDS directly. PopHydra Optimizer is distinctive in its distinctive hybrid architecture, which is a combination of the Poplar Optimization Algorithm and the Waterwheel Plant Algorithm. With the combination of these two algorithms, PopHydra Optimizer can explore and optimize a good number of parameters in the decision-making process, especially the discount factor, to high precision and flexibility. Two-algorithm architecture significantly improves the model's responseability to dynamic and evolving patterns of attacks in IIoT-SCADA systems.

PopHydra Optimizer is especially well-suited to calculate discount factors since it utilizes an intrinsic approach of optimization, where it changes model parameters. A discount factor is used in reinforcement learning to value future rewards as opposed to present rewards. Suboptimal learning, where the model overestimates present rewards or overlooks the long-term impact of choices, is a result of an ill-optimized discount factor. PopHydra optimization in hybrid ensures that the factor is optimized to the point that the IDS system makes more reasonable decisions in the long term regarding threats. This allows the system to identify complex dynamic cyber threats with better efficiency in real time. PopHydra Optimizer ensures that the IDS can weigh present and future factors with greater accuracy, thereby improving both the detection rate and accuracy while effectively blocking IIoT attacks. One of the major strengths of PopHydra Optimizer is its dynamic capacity to learn from the growing nature of threats in IIoT-SCADA systems. Threats continually evolve, and traditional IDS models struggle to maintain high detection rates due to the increasing complexity of attacks and their mechanisms over time. Using evolution algorithms and liquid-based methods to continuously adjust the discount factor, PopHydra Optimizer helps the IDS model work well and quickly against even new and unknown attacks. The dynamic optimization technique aids in threat mitigation by effectively reducing associated risks, such as those posed by zero-day attacks or Advanced Persistent Threat (APT)-type attacks. This approach requires the system not only to detect but also to predict and respond to emerging threats. Real-time performance-based optimization via PopHydra Optimizer further allows for optimality in responses through the performance of IDS systems, enabling humongous data handling on IIoT devices without waste or delay and which is majorly essential on latency-dependent systems.

4 Results and Discussions

The three datasets used to test the proposed model are well-established, robust, and relevant to several different IoT environments, which nicely makes a case for the proposed model's performance. The dataset CICIoT2023 [18] specifically employs the methods typically used to collect network traffic in smart home environments, accurately capturing the normal conditions expected in such an IoT setting. WUSTL-IIoT [19,20], generated by Washington University in St. Louis, focuses on the IIoT and has been crafted to serve as a tool for improving intrusion detection in the unique operational contexts of the IIoT. Finally, UNSW-NB15 is a widely used and popular dataset for network intrusion detection. It serves to help emulate modern network environments, with a blend of normal and malicious activities, everything from reconnaissance to DoS to SQL injection, that one would hope to encounter when wading through a real-world network. It's a dataset that proffers a pretty sweet, general view of network traffic and is hence well-suited for testing the overall performance of any model in telling good traffic from bad across a diversely blended mix that a real-world network would hope to encounter.

The CICIoT2023 dataset involves different types of attacks; it offers an opportunity for fine-grained analysis of attack patterns, especially for understanding associations between those patterns. For this type of understanding, we can use a method known as co-occurrence analysis. This method involves looking at whether two or more attack types tend to occur at the same time within the same networked instance. As shown in Fig. 2, a close look at the instances within the dataset where these two attacks co-occur reveals that the attackers seem to use these two methods together in an attempt to take down the target. The CyberFortis model's effectiveness at detecting intrusion classes is gauged through the metrics of precision, recall, and F1-score, as shown in Fig. 3.

Precision describes how many of the predicted positive cases were actually correct. In the case of CyberFortis, this refers to the number of predicted intrusions that were actually correct. Recall is a way of measuring how effective the model is at catching all the actual positive cases. For CyberFortis, that means how well it is doing at catching all the actual intrusions. A low recall value, in this context, would indicate that many successful intrusions occurred without detection. In the same way, the F1 score is used to average together precision and recall. When all three of these metrics were examined together, they appeared to indicate that the CyberFortis model is successful at detecting many different types of intrusion.

There are additional analyses of the model performance through the False Positive Rate (FPR) and False Negative Rate (FNR) in Fig. 4. This is important in understanding the tradeoff between correctly classifying the benign and the real malicious traffic. FPR is driven by the amount of benign traffic that is misclassified as malicious, while FNR is concerned with destructive traffic that is wrongly deemed as benign. For the CyberFortis model, a general observation about the FPR is that it remains very low across all of the attack classes. The highest average value of FPR is 0.0111, which is recorded for the DDoS attack, and the lowest, on the other hand, is 0.0001, which is recorded for Benign traffic. The FNR values, on the other hand, are rather moderate, where the highest FNR value is in Recon attacks at 0.0473 and the lowest for BruteForce at 0.0012.

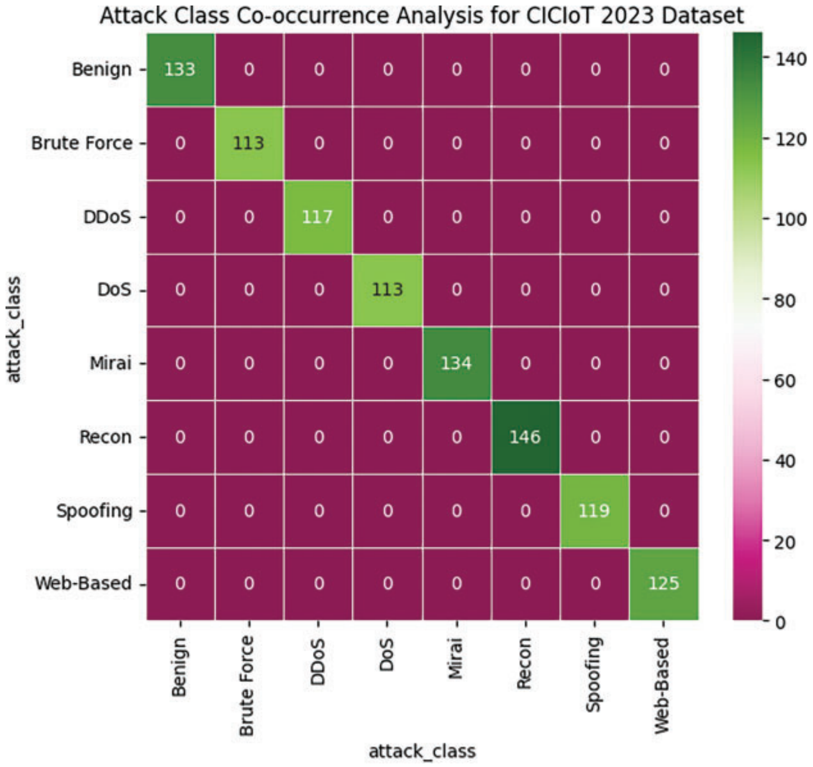

Figure 2: Co-occurrence analysis for CICIoT 2023 dataset

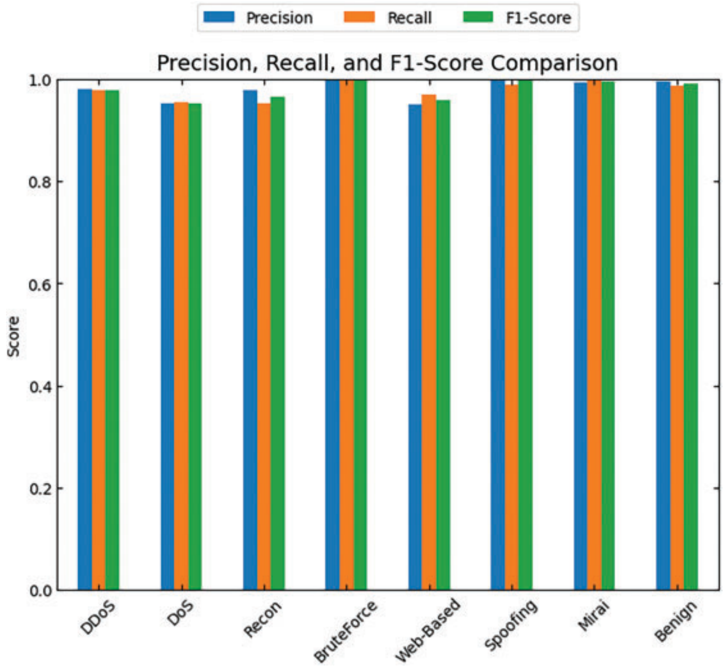

Figure 3: Precision, recall and f1-score analysis of the proposed CyberFortis model with respect to different classes of intrusions

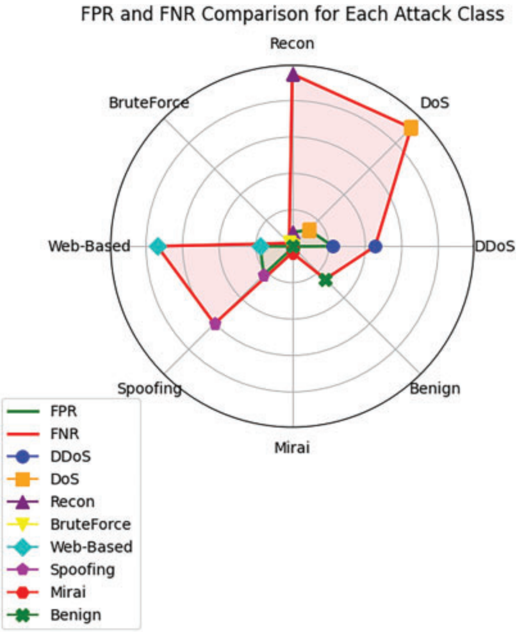

Figure 4: FPR and FNR analysis of the proposed CyberFortis model with respect to different classes of intrusions

The model is most sensitive to Mirai (0.0018) and Spoofing (0.0301) attacks. These attacks are, for some reason, more likely to be detected as if they are intrusions, meaning that there are fewer chances of false negatives. Overall, the FPR and FNR analysis have shown that CyberFortis is successful in restraining too many false positives and too many false negatives, distinguishing it as a credible model for intrusion detection in different cyberattack situations. The proposed framework's performance comparison with other security frameworks in Fig. 5 shows the proposed model's capability of detecting intrusions with the UNSW-NB15 dataset, which contains multitudes of different network traffic data and is commonly used for comparing the effectiveness of an IDS. Another strength of the model is its precision score, which measures the accuracy of positive predictions, and it stands at 98.9%. This score is significantly better than other competing models' precision scores, like Deep Neural Network (VAE) at 95.2% or Deep Neural Network (DNN), which is at 62%. This all means that the proposed model is more effective at reducing false positives and more accurate at flagged intrusions. The Proposed model comes out ahead of the rest with an F1-score of 98.89%, which all other models also fail to achieve.

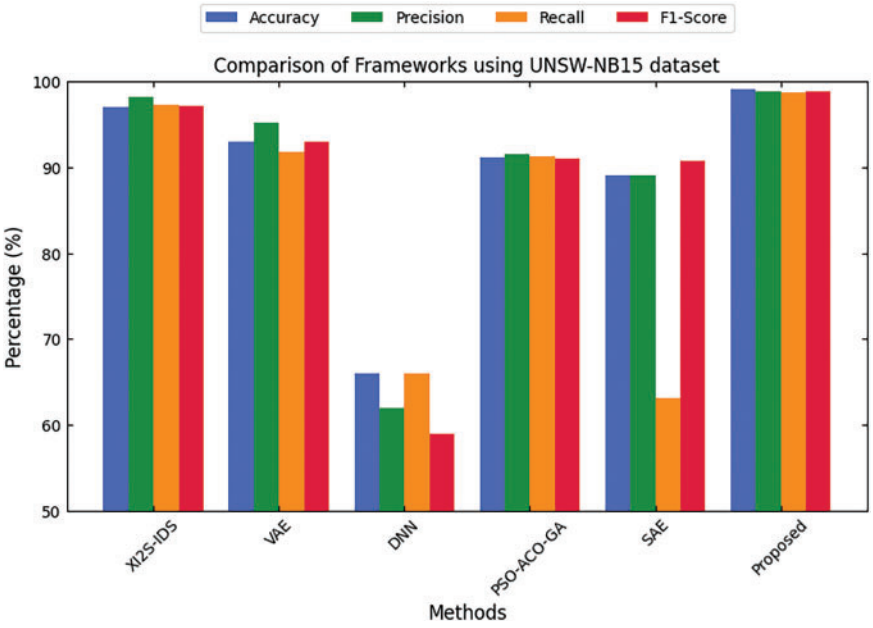

Figure 5: Comparison with other security frameworks using the UNSW-NB15 dataset

Fig. 6 gives a complete evaluation of different techniques with reference to performance metrics such as accuracy, precision, recall, and F1-score on the WUSTL-IIoT dataset. Comparison results show that the proposed model has greatly excelled in performance amongst almost all metrics considered over other well-recognized methods, including XGBoost + DT, Optimized GRU, INB–PCA, iForest, and OIFIDS. Starting with accuracy, the proposed model gives an exhaustive performance of 97.5%, which is well above all others; in contrast, OIFIDS achieves up to 94.8%, and iForest obtains the minimum, with an accuracy of 84.2%. With respect to recall, the proposed model obtains a performance of 97.5%, again standing out against iForest's performance of 78% and XGBoost + DT with 98.38%. F1-score, the harmonic mean between recall and precision, also endorses the fantastic performance of the proposed model.

Fig. 7 illustrates the analysis of the False Positive Rate for different techniques on the WUSTL-IIoT dataset. With an FPR value of 0.9, the proposed model achieves the lowest False Positive Rate, making it the most effective among the various techniques in avoiding false positives. On the other hand, Optimized GRU and INB-PCA have FPR values of 6 and 3.9, respectively, suggesting that these techniques are not as effective in distinguishing between benign and malicious traffic. XGBoost + DT, iForest, and OIFIDS register moderate FPR values under 2.4. This proves the superiority of the proposed model in terms of reducing false alarms, hence confirming its suitability for intrusion detection in IIoT environments.

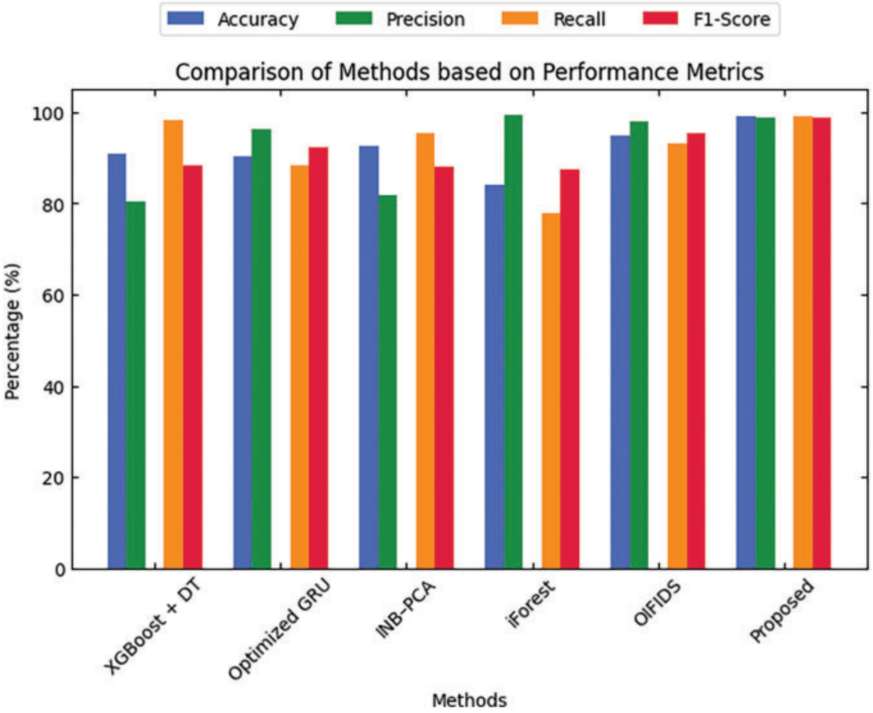

Figure 6: Comparison of methods based on performance metrics using the WUSTL-IIoT dataset

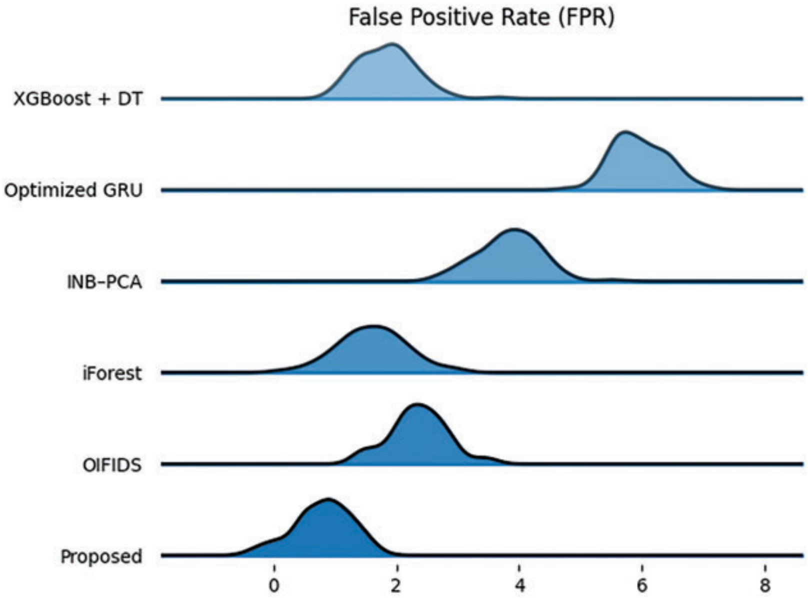

Figure 7: FPR analysis using the WUSTL-IIoT dataset

Fig. 8 shows the feature of accuracy comparison of different techniques that make use of UNSW-NB15 as a dataset. The proposed model stands out by achieving the highest accuracy of 97.5%, demonstrating its ability to classify benign and malignant traffic with strong confidence. In contrast, the Ensemble technique yields a mere 87.33%, which is the least compared to the others. The other models, like Optimized Gate Recurrent Unit (GRU) and multi-scale adversarial network with attention (MSANA), show reasonably close accuracies of about 88% and 89.4%, respectively, implying that the effectiveness is observed but does not exceed the capability of the proposed model.

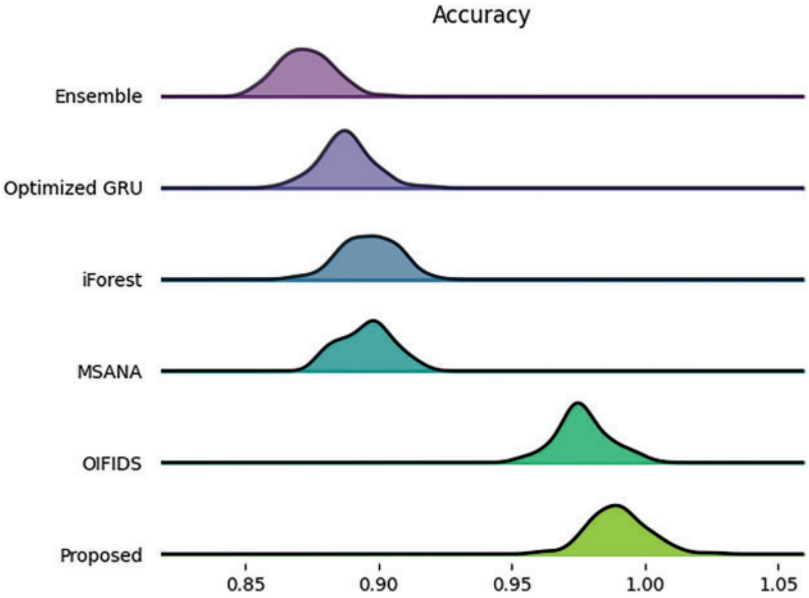

Figure 8: Accuracy comparison using UNSW-NB 15 dataset

Fig. 9 compares the different models based on precision. The model proposed is again ranking at 98.9%, implying both significant identification of the positive tokens while keeping the false positive rates low. OIFIDS follows closely with a considerably lower precision score of 91.53%, which indicates that the classifier performs well, although it is not on par with the proposed model. Based on the precision scores relative to the model proposed, concerning iForest and in the case of the Optimized GRU, they show somewhat lower levels of precision score, indicating the high likelihood of False positives in the models compared to that of the proposed technique. Fig. 10 presents recall figures from different models for the same experiments. The proposed model again outperforms, yielding a recall of 97.5%, meaning it has the ability to identify practically all positive examples in the dataset. OIFIDS takes second place, yielding a recall of 97.4%, still putting it in close water with regard to sensitivity toward malicious instances. The others, on the other hand, Ensemble, MSANA, and Optimized GRU, happen to show themselves a bit weaker with recall values rating from 94% to 96%, which reverts its detection capability for some intrusions being quite less in comparison with the proposed model.

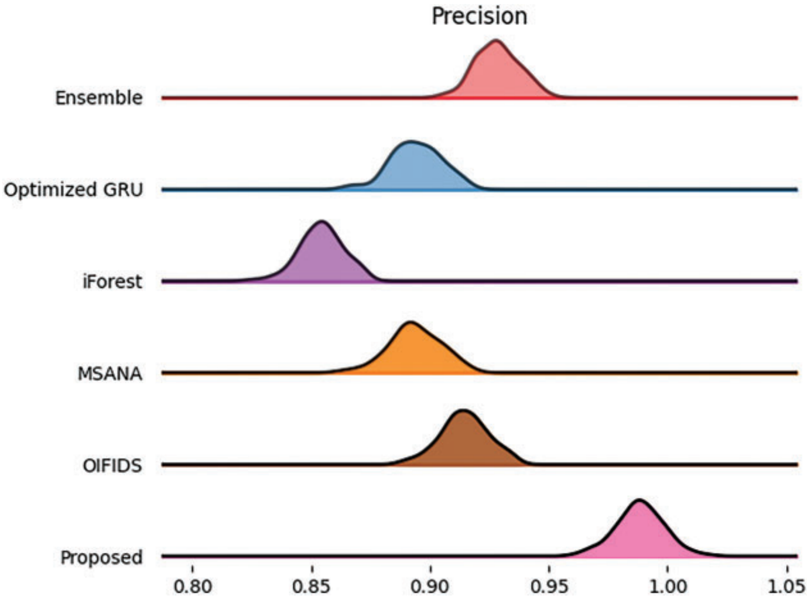

Figure 9: Precision comparison using the UNSW-NB 15 dataset

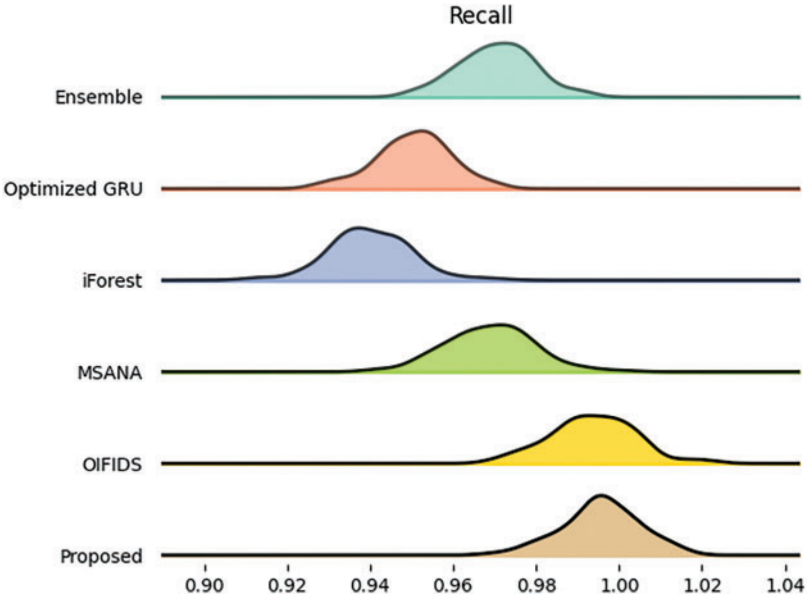

Figure 10: Recall comparison using the UNSW-NB 15 dataset

5 Conclusion

This paper presents a comprehensive study of their improvement in the intrusion detection of IIoT-SCADA systems by suggesting two different approaches. These are SiamDQN-AE FusionNet for Intrusion Detection and PopHydra Optimizer for Discount Factor Computation. The proposed SiamDQN-AE FusionNet is an entirely novel architecture that effectively employs a novel combination of Siamese DQNs with the reduced-level solutions of AEs to achieve effective detection of a variety of attacks in complex IIoT environments. Also, together with PopHydra Optimizer, it provides an innovative take on discount factor computation in reinforcement learning and thereby speeds up the convergence of the network and makes it more efficient. As such, decision-making is thus considerably strengthened. The novelty and contribution of this work thus build on the elucidation of the deep reinforcement learning and autoencoder approach, which has not been thoroughly examined earlier in the context of IIoT-SCADA systems. The proposed model achieved an impressive 97.5% accuracy and nearly 97% in F1-score evaluation, demonstrating its strength and effectiveness. The proposed model renownedly achieved 97.5% accuracy and close to 97% in F1-score appraisal, proving its strength and efficacy. It also indicates that advanced deep learning architecture and optimization techniques have significant roles in improving the capabilities of intrusion detection in industrial environments, thus being the impetus for guaranteeing security and resiliency for IIoT-SCADA systems amidst expanding cyber risks.

Acknowledgement: The authors extend their thanks to the Ongoing Research Funding Program (ORF-2025-846), King Saud University, Riyadh, Saudi Arabia.

Funding Statement: This work is financially supported by the Ongoing Research Funding Program (ORF-2025-846), King Saud University, Riyadh, Saudi Arabia.

Author Contributions: Conceptualization, Kuncham Sreenivasa Rao, Rajitha Kotoju and B. Ramana Reddy; methodology, Kuncham Sreenivasa Rao, Rajitha Kotoju and B. Ramana Reddy; software, Subhav Singh and Shitharth Selvarajan; validation, Taher Al-Shehari and Nasser A. Alsadhan; formal analysis, Subhav Singh and Shitharth Selvarajan; investigation, Taher Al-Shehari and Nasser A. Alsadhan; resources, Subhav Singh and Shitharth Selvarajan; data curation, Subhav Singh and Shitharth Selvarajan; writing—original draft preparation, Kuncham Sreenivasa Rao, Rajitha Kotoju and B. Ramana Reddy; writing—review and editing, Taher Al-Shehari and Nasser A. Alsadhan; visualization, Taher Al-Shehari and Nasser A. Alsadhan; supervision, Subhav Singh and Shitharth Selvarajan. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The datasets used and analysed during the current study are available from the corresponding author on request.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Dildar MS, Khan AS, Abbasi IA, Shaheen R, Al Ruqaishi K, Ahmed S. End-to-end security mechanism using blockchain for Industrial Internet of Things. IEEE Access. 2025;13(5):20584–98. doi:10.1109/access.2025.3535821.
2. Saied M, Guirguis S, Madbouly M. Review of filtering based feature selection for Botnet detection in the Internet of Things. Artif Intell Rev. 2025;58(4):119. doi:10.1007/s10462-025-11113-0.
3. Shang W, Ding L, Yang X, Gu Z, Sui H. Complicated imbalanced and overlapped data oversampling approach via hypersphere coverage and adaptive differential evolution for anomaly detection of Industrial Internet of Things. IEEE Internet Things J. 2025;12(10):14002–15. doi:10.1109/jiot.2025.3526160.
4. Ahakonye LAC, Nwakanma CI, Lee JM, Kim DS. Trees bootstrap aggregation for detection and characterization of IoT-SCADA network traffic. IEEE Trans Ind Inform. 2023;20(4):5217–28. doi:10.1109/tii.2023.3333438.
5. Abdullahi SM, Lazarova-Molnar S. On the adoption and deployment of secure and privacy-preserving IIoT in smart manufacturing: a comprehensive guide with recent advances. Int J Inf Secur. 2025;24(1):53. doi:10.1007/s10207-024-00951-8.
6. Termanini A, Al-Abri D, Bourdoucen H, Al Maashri A. Using machine learning to detect network intrusions in industrial control systems: a survey. Int J Inf Secur. 2025;24(1):20. doi:10.1007/s10207-024-00916-x.

7. Ahakonye LAC, Nwakanma CI, Lee J-M, Kim D-S. SCADA intrusion detection scheme exploiting the fusion of modified decision tree and Chi-square feature selection. Internet Things. 2023;21(9):100676. doi:10.1016/j.iot.2022.100676.
8. Babayigit B, Abubaker M. Industrial Internet of Things: a review of improvements over traditional SCADA systems for industrial automation. IEEE Syst J. 2023;18(1):120–33. doi:10.1109/jsyst.2023.3270620.
9. Mishra S, Anithakumari T, Sahay R, Shrivastava RK, Mohanty SN, Shahid AH. LIRAD: lightweight tree-based approaches on resource-constrained IoT devices for attack detection. Clust Comput. 2025;28(2):1–23. doi:10.1007/s10586-024-04792-x.
10. Yalçın N, Çakır S, Üaldı S. Attack detection using artificial intelligence methods for SCADA security. IEEE Internet Things J. 2024;11(24):39550–9. doi:10.1109/jiot.2024.3447876.
11. Gueye T, Wang Y, Rehman M, Mushtaq RT, Zahoor S. A novel method to detect cyber-attacks in IoT/IIoT devices on the Modbus protocol using deep learning. Clust Comput. 2023;26:2947–73. doi:10.21203/rs.3.rs-1762940/v2.
12. Zainudin A, Akter R, Kim D-S, Lee J-M. Federated learning inspired low-complexity intrusion detection and classification technique for SDN-based industrial CPS. IEEE Trans Netw Serv Manag. 2023;20(3):2442–59. doi:10.1109/tnsm.2023.3299606.
13. Srinivasan M, Senthilkumar N. Intrusion detection and prevention system (IDPS) model for IIoT environments using hybridized framework. IEEE Access. 2025;13(15):26608–21. doi:10.1109/access.2025.3538461.
14. Benka D, Horváth D, Špendla L, Gašpar G, Strémy M. Machine learning-based detection of anomalies, intrusions and threats in industrial control systems. IEEE Access. 2025;13:12502–14. doi:10.1109/access.2025.3530902.
15. Zeng GQ, Yang YW, Lu KD, Geng GG, Weng J. Evolutionary adversarial autoencoder for unsupervised anomaly detection of Industrial Internet of Things. IEEE Trans Reliab. 2025:1–15. doi:10.1109/tr.2025.3528256.
16. Bansal K, Singhrova A. Review on intrusion detection system for IoT/IIoT-brief study. Multimed Tools Appl. 2024;83(8):23083–108. doi:10.1007/s11042-023-16395-6.
17. Sangoleye F, Johnson J, Tsiropoulou EE. Intrusion detection in industrial control systems based on deep reinforcement learning. IEEE Access. 2024;12(1):151444–59. doi:10.1109/access.2024.3477415.
18. Vulfin A. Detection of network attacks in a heterogeneous industrial network based on machine learning. Program Comput Softw. 2023;49(4):333–45. doi:10.1134/s0361768823040126.
19. Eid AM, Soudan B, Nassif AB, Injadat M. Comparative study of ML models for IIoT intrusion detection: impact of data preprocessing and balancing. Neural Comput Appl. 2024;36(13):6955–72. doi:10.1007/s00521-024-09439-x.
20. Babayigit B, Abubaker M. Towards a generalized hybrid deep learning model with optimized hyperparameters for malicious traffic detection in the Industrial Internet of Things. Eng Appl Artif Intell. 2024;128(2):107515. doi:10.1016/j.engappai.2023.107515.