International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Protecting Software Defined Networks with IoT and Deep Reinforcement Learning

Mahmoud Abou Ghaly*[1], Shaikh Abdul Hannan[2]

Submitted: 11/10/2023 **Revised**: 30/11/2023 **Accepted**: 11/12/2023

Abstract: The Internet of Things (IoT) has been seeing rapid expansion for a reason that is quite justifiable. The operators of these devices have already put up a diligent infrastructure. Among the technologies that need to be created to support this kind of sensors are enterprise safety initiatives. This paper discusses the stability routing protocol, which is based on a trustworthy assessment of the equipment and packet flow. To build trustworthy Software-Defined a network (SDN) routes, improve the trust in network a part moves and the Quantity of Service, or QoS, or power conditions. When utilized alongside deep learning algorithms, the DRL-IDS structure described in this the work successfully identifies hacking. It is based on a feature selection technique based on LightGBM, which successfully decides on the most appealing set of characteristics from company Internet of Things data. The application depends on GBM's selection of features system, which takes industrial Internet of Things knowledge and extracts the most compelling feature set; the multilayer perception network's hidden layer is then used along with the deep learning algorithm to create the prevalent network architecture for the valuable network and significant system in the PPO2 algorithm; and lastly, the PPO2 method and ReLU (R) technology are used to create the breach detection model. Comprehensive evaluation on a publicly available data set demonstrates that the proposed system for intrusion detection is 95 percent accurate in identifying different kinds of network attacks within the Sector the internet of Things. The currently the system is used for detection of intrusions is based on models using deep learning such as LSTM, CNN, and RNN, and extensive reinforcement programming algorithms like DDQN and DQN.

Keywords: *Internet of Things (IoT), Software-Defined Network (SDN), LightGBM, Multilayer Perception Network, Deep Reinforcement Learning.*

1. Introduction

Recent advancements in digital transformation and new technologies have expanded the scope of information access technologies. Technologies such as big data, computing on the edge, learning algorithms, and the Internet of Things (IoT) are undergoing rapid change. The Internet is becoming more and more integrated into people's lives, which presents a range of varied and intricate risks to data and further fragments security operations. Many IoT devices have generated a lot of data, and in the future, there will be an even greater variety and quantity of these devices. It is possible that conventional IoT systems are ill-prepared to deal with the challenges this presents. [1]

The fragmentation of safety standards and situations has been one of the main issues facing Internet security in recent times. Furthermore, it's growing more difficult to overlook the differences between commercial settings and security assets. Put differently, lowering expenses is the most significant issue confronting enterprises today as the quantity and variety of Internet of Things (IoT) devices and safety precautions continue to grow at an accelerated rate. However, the disparity between business circumstances and security measures is a major issue with cost optimization. [2]

The Crucial Guidelines for Data Protection and Security Infrastructure draws attention to the security issues and fundamental security requirements that vital information infrastructure must satisfy. To realize the protection concept, involving everything from capability planning to coordinated response, monitoring of the global situation, building an active, proactive, adaptable, and receptive safety protection framework with a Security Middle Platform (SMP) at its core is necessary. Walled defense, the traditional approach, is inadequate to deal with them. [3]

The term "Industrial Internet of Things" refers to the application of Internet of Things technology inside the manufacturing industry. The primary objective is to facilitate the development and seamless integration of Internet of Things (IoT) and industrial automation technologies. The Commercial Network of Things has facilitated unprecedented degrees of interconnection among production, supervisory, and administration subsystems, which were previously unattainable. The control center encompasses a multitude of diverse systems. The

*[*1] IT Department, Faculty of Computing and Information, Al-Baha University, Al-Baha, Kingdom of Saudi Arabia.*
*[*1] Mathematics Department, Faculty of Science, AinShams University, Cairo, Egypt.*
[2] Department of Commuting and Information, Al-Baha University, Al-Baha, Kingdom of Saudi Arabia.
Corresponding Author : abdulhannan05@gmail.com

implementation of unified management systems enhances the operational efficiency in the processing of diverse industrial data. The manufacturing sector's implementation of the Internet of Things (IoT) is encountering a rise in network security vulnerabilities due to its intricate nature and inherent connectivity.

In 2019, the CNCERT, the National Internet Security Centre, published a situation review that revealed high-risk weaknesses and hidden hazards in approximately 41% of the Manufacturing Internet of Things devices. 2653 sets of electrical power, 584 sets of natural gas and petroleum, and 100 sets of commuter rail were among the 2249 sets of networking control and administration systems that were found to be exposed in important industries, including the oil and gas, urban rail transit, and electricity. Network complexity is a challenge for industrial IoT [4]. The system as a whole could be severely harmed very quickly by any malfunction or anomaly in one of its components. For a prompt and efficient network response, it is therefore essential to identify network attacks with speed and accuracy [5].

Inspired by Software-Defined Safety (SDSec) and the Security Middle Platform (SMP), the software-defined security depends system structure (SDSmp), as shown in Figure 1, is built for the whole scenario.

The goal is to find solutions for low utilization, challenging resource reuse, and highly fragmented security scenarios and requirements in order to cut costs. Additionally, the SDSmp offers a workable focal point to address the mismatch issue between company situations and security-related means, enhancing the adaptability and capacity of security protection.

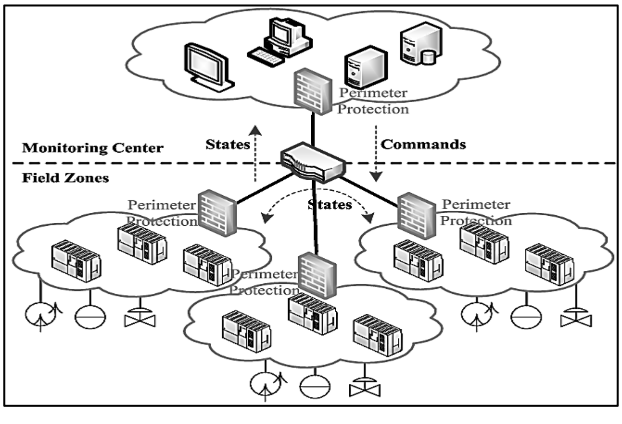


Fig. 1 Middle Platform Architecture for Software-Defined Security [5]

We added the management of security circuits after realizing how crucial navigation is to stopping attacks on computer systems. Serving as a vital part of SerIoT, or Secure or Reliable Wireless Computing. Works with others to develop novel channel management strategies for SDN networks, with a primary emphasis on online perception security monitoring and reveal [6].

Compile a lot of security information or know which automobiles or hubs have their coverage restricted so that pedestrians suspected of being part of a cyberattack are sent to a less critical alert. Changing the protected trails or getting rid of the server are two examples of altering trail management depending on stability.

The goal is to increase the level of assurance for network consumer or network provider devices by achieving enhanced durability attacks in response to recently developed techniques or methodologies. Penetration testers are a relatively new and skilled innovation, which is one reason for the emphasis on SDN's significant advancement in research or implementation.

A review of different programs financed the European Commission is included in a pertinent present research paper on cybercrime throughout Europe [7].

All facets of information systems are severely hampered by cybercrime for mobile communications. The majority of contemporary mobile devices allow users to connect to Wi-Fi through other cellular routers; however, new security features that control network traffic should be constantly observed and taken into account when designing Smartphone apps.

As a result, a prior survey looked at how computer vision and Artificial Neural Networks (ANNs) might be used to solve this issue. Attacks on the airplane that activate the foundation network are the subject of research because they directly affect the provider of mobile services or the final user. By utilising queuing theory methodologies, the NEMESYS initiative was able to overcome numerous challenges.

This study examines the safety aspects pertaining to communication and information transmission routes within European medical systems, namely those operating at the national or regional level.

Health computing platforms should have sufficient virtual patient records available for European travellers who require medical care outside of their continent. The design of a dependable home central server is the main topic of this article, which also addresses protection in the home IoT industry.

The high cost of emerging safety crises makes it difficult for the safety industry to handle. A DRL-based method for real-time pricing optimization of the Multi-Party Computing Software Defining Secure Middle Platforms (MPC-SDSmp) is presented in order to work around the aforementioned concerns. In-depth instructions are provided for creating and implementing algorithms, and a thorough evaluation of effectiveness is carried out using extensive simulations of various load kinds.

We have put a lot of efforts into reducing the SDSmp's cost in order to solve the Software-Defined Security (SDSec) optimization cost issues. The contributions made are compiled in the sections that follow:

- From an architectural standpoint, it lowers deployment costs through increased resource reuse for security infrastructure and optimized architecture. Specifically, SDSmp proposes an automated control building for divided security scenarios and demands, accomplishes mechanical resource management and immediate planning, and isolates the security facilities both geographically as well as electronically using the cloud for computing and network operation virtualization. Multi-Party Computing (MPC) ensures that the authentication layer of apps is data agnostic and protects the privacy of users from leaks by building Smp, which enables the reuse of resources in secure architecture.
- In terms of modelling, a DRL-based SDSmp cost optimization algorithm is created so that the control plane's intelligent scheduler can acquire the ability to choose Smp resources sensibly based on actual usage. This results in low response times, load balancing, and high quality-of-service satisfaction while lowering operating costs [8].
- An SDSmp experimental environment is constructed for practical use. The proposed DRL-based approach for real time optimization of the prices of MPC-SDSmp has been contrasted with existing real-time job-scheduling algorithms under different workload scenarios. The experimental results show that the proposed method outperforms existing immediate solutions with regard to of cost, quality of service, load balancing, and overall reaction time [9].

This article's intrusion detection system was evaluated as an organizational outcome employing the Industry Internet of Things data set that the US Department of the Energy's Oak Ridge National Laboratory made accessible to the public. The findings demonstrate the effectiveness of the intrusion detection system [10]. He prevented 99.9% of the different kinds of cyberattacks.

A. Objective of the study

- Investigate how IoT devices might be integrated into SDNs for a range of uses, including network management, data collection, and monitoring.
- Evaluate the viability and efficacy of the suggested IoT and Deep Reinforcement Learning-based security approaches within SDNs through real-world case studies or simulations.

2. Related Work

A world where billions of connected devices are placed practically [11] everywhere—from the innards of human beings to the furthest edges of the earth—is made conceivable by the Internet of Things (IoT). It is now more important than ever to address the huge security threats associated with the Internet of Things (IoT), as it will soon be easily accessible from anywhere. Conventional methods that treat security as a last-minute consideration and a "patch" for acknowledged weaknesses are inadequate. In fact, a new secure-by-design paradigm will be needed to meet the challenges of the next generation of IoT, one in which threats are proactively addressed and IoT devices are trained to rapidly adapt to varying threats. Consequently, Software-Defined Networking (SDN) and Machine Learning (ML) will be essential for giving Internet of Things (IoT) devices intelligence and configurability .

The Internet of Things (IoT) [12] is currently experiencing massive data streaming as a result of the widespread use of smart devices. The requirements of computing-intensive but delay-sensitive applications, however, are beyond the capabilities of the resource-constrained devices. Malevolent users may manipulate the way data is delivered between devices. These create new obstacles in the way of delivering intelligent and safe IoT services. Two techniques that show promise for creating an atmosphere of safety and intelligent utilization of resources are block chains and Reinforcement Learning(RL). In this paper, we present a new edge-cloud orchestrated computing architecture enabled by Software Defined Networking (SDN) to enable safe and smart IoT services.

Software-Defined Networking (SDN) [13] is an unprecedented breakthrough in the field of networking with many appealing attributes, including management and flexibility. Despite these advantages, SDN is susceptible to Distributed Denial of Services (DDoS) assaults, which entail a significant risk due to the harm they may do to the SDN system. Even with a variety of security techniques, DDoS attack detection is still an open research problem. In order to thoroughly research and critically evaluate the current DDoS attack strategies that utilize Artificial Intelligence (AI), Machine Learning (ML), Deeper Learning (DL), or combination methods released between 2014 and 2022, this study provides a Systematic Literature Review (SLR).

In this paper [14], accurate anomaly identification is ensured by the recursive design of networks used for traffic flow monitoring. By using the proposed method, cyberattacks in SDN become more effective. The proposed model prevents network forwarding performance degradation, which allows it to achieve an impressive attack detection performance against Distributed Denial-Of-Service (DDoS) attacks. By proactively safeguarding the

SDN data layer from overload, the recommended methodology aims to educate users on how to adapt to the flow of traffic in methods that yield greater granularity. Applying a learned traffic flow match control policy improves the effectiveness of cyber-attack detection by enabling the acquisition of optimal traffic data for identifying irregularities during runtime.

Personalized health care [15], cities with AI and smart grids, the military, and agriculture are just a few of the industries utilizing the Internet of Things (IoT). Important infrastructures are also controlled by it. All the same, malware attacks can occur on IoT devices because they lack security protocols and the capacity for processing to run computationally intensive anti-malware apps. Furthermore, known malware fingerprints kept in their database are the traditional means by which virus-detection mechanisms recognize a threat.

A significant amount of research [16] has been done on the security of Software Defined Networks (SDNs) in order to support their diverse applications. SDNs are becoming a more cutting-edge innovation in the network space. The study initially focuses at the state-of-the-art in SDN safety from a data viewpoint. Following that, a few common techniques for Networks Attacks Detection (NAD) are reviewed, including statistics and machine learning-based techniques. After that, Tensor Principal Components Analysis (TPCA), a novel tensor-based technique for network attack detection, is suggested. After a review of the most current data-driven SDN frameworks, a tensor-based big based on data SDN detecting framework is recommended for SDN security. Lastly, a real-life example is provided to confirm the usefulness of the suggested framework.

Due to the growing [17] demands on device heterogeneity brought about by the Internet of Things (IoT) and the continually changing traffic demands of next-generation applications and services, managing contemporary network environments is getting more and more difficult. Software-Defined Networking (SDN) is a management paradigm that can handle this issue by using a centrally managed high-level network approach. But since the main controller can be attacked by hostile users looking to disrupt network operations, this centralized feature also generates a critical failure point. This paper presents an SDN defined system that detects DDoS and intrusion attempts using the Gates Recurrent Unit (GRU) deep neural network method that utilizes the analysis of individual IP flow records.

The ground-breaking concept of the Software Defining Network (SDN) [18] allows control and data planes to be separated to create a software-driven network. SDN essentially fixes the issues that the conventional network architecture had; nevertheless, it might also make the network more vulnerable to fresh threats. Distributed denial of Service (DDoS) assaults is among the most difficult to stop in these software-based networks. The performance of current DDoS mitigation techniques is either inadequate or compromises the accuracy of attack detection. We suggest an automatic learning-based DDoS mitigation method for SDN in this paper to close the gaps. The NSL-KDD dataset is used to first build an algorithm to DDoS detection in SDN. Following model training on this dataset, real DDoS attacks are used to evaluate our suggested model.

The study [19] uses deep learning techniques for implementing a new SDN in IoTs. Initially, the DBN was used to extract useful malware features from the input data. Only two RBM were used in this study's DBN, depending on how big the input features were. The DBN's features extracted were classified using a relatively shallow neural network. In order to identify the malware, we used a shallow neural network, and the outcomes were different from a shallow neural network based on DBN. The shallow neural network based on DBN outperformed the shallow neural network in terms of results.

Wireless Networks of Sensors (WSNs) [20] have limited resources and an open transmission medium, they are highly vulnerable to persistent security threats. Hundreds of thousands of resource-constrained, self-organizing sensor nodes make up a WSN. Since these nodes with sensors are typically arranged in a distributed fashion, it is possible to create a network of these devices without the need for central administration or established infrastructure. The challenge that comes with gaining control over real-time applications by WSNs—where malicious activity has the potential to cause significant harm—is strengthening security enforcement within these networks. Software-Defined Networks (SDN) has been developed as a remedy, and it has been combined with Wireless Sensor Network (WSN) to create Software-Defined Wireless Sensors Network (SDWSN).

3. Methodologies

3.1. System for Detecting Intrusions Using Deep Reinforcement Learning (DRL).

The data processed component, the intrusion prevention agent (agent) emergence module, and the infiltration detection agent learning module make up the three primary elements of the PPO2-based attack detection system DRL-IDS that is presented in this study (see Figure 2). The detection of invasions agent construction module simply consists of setting training methods, building value functions, and determining the external environment phase model of learning via reinforcement; the analysis component is made up of picking features and preliminary processing data [21].

The environment in the state model is the confidential presentation of the environment that is concealed from an intrusion detection system and leaves out the domain that establishes the rules for reward and punishment.

The intrusion detecting agent's action decision strategy is further optimized by the training strategy, which assesses the value function and updates its parameters based on feedback from the state of the environment model's punishment and reward (loss function) systems. The intrusion detecting agent's training module keeps using the loss function to optimize the system until the model convergence occurs or finishes the designated.

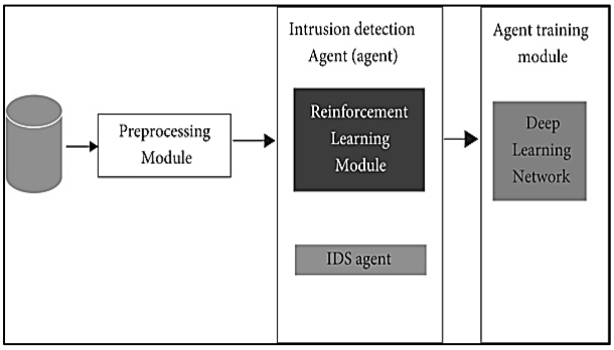


Fig. 2 System for Detecting Intrusions Using Deep Reinforcement Learning [21]

3.2. Module for Data Processing

In order to reduce noise in the background duplicate of the initial data input and improve the model's efficiency in detecting multiple classes, the intrusion detection approach utilized in this study first identifies aspects.

Assuming that intrusion detection efficiency is guaranteed, it effectively reduces the data's reliability aspect [22]. Embedding is the cornerstone of the intrusion detection system. The choice of features algorithm of the formula for the LightGBM as algorithm performs feature screen using the following particular tactics:

(a) Features that have missing values in excess of 60% of the thresholds should be eliminated (a). Experience has shown that this feature has little bearing on how intrusion detection agents are trained when the missing rate exceeds 60%.

(b) Eliminate the feature's unique value.

(c) In every feature pair with a strong correlation, remove any feature. The Pearson correlation coefficient of 0.99 is the specific thresholds (absolute value) for the highly correlated feature pair.

(d) Use the LightGBM algorithm to remove the features that have a lower importance ranking [23]. Until the model's performance stops improving, the final feature count will progressively increase features in the feature importance score order.

(e) To equalize the parameters in different intervals, the range's characteristic numbers are scaled to the interval [0, 1] using the most basic min-max function. The following equation displays the precise formula:

$$S' = \frac{S-\min(s)}{Max\ (s)-\min\ (S)}. \qquad \textbf{...1}$$

$$T_f^{ANA} = T_{t,f}^{l} + T_{c,f}^{l} + T_f^{FB}. \qquad \textbf{...2}$$

$$T_f^{ANA} = T_{t,f}^{l} + T_{c,f.}^{l} + T_{t,f}^{l-cloud} + T_{c,f}^{cloud} + T_{f.}^{FB}.. \qquad \textbf{...3}$$

$$T_f^{ANA} = T_{t,f}^{cloud} + T_{c,f}^{cloud} + T_f^{FB}. \qquad \textbf{...4}$$

$$t_n^f = \frac{b}{c_{i,j.}}. \qquad \textbf{...5}$$

$$EIP_{i,j}^f = \frac{N_F.t_{max}}{t_n^f}.$$

...6

$$C_t = R_{t+1} + \alpha R_{t+2} + \cdots + \alpha^m R_{t+m+1} = \sum_{m=0}^{\infty} \alpha^m R_{t+m+1}$$

...7

3.3. Construction of Value Functions

The anticipation of rewards, or value function, is primarily utilized to assess the relative merits of various states and direct the agent's behaviour [24] . The information that can affect the agent's judgment for the next course of action is included in the agent's state.

3.4. Definition of a Training Strategy

The mapping state to action is a malware prevention system training approach. DRL-IDS uses the PPO2 algorithm, which was suggested by the company DeepMind and OpenAI. The local optimum algorithm TRPO, who is more flexible, sophisticated, and uncomplicated than TRPO and PPO2, is the basis for this algorithm.

Additionally, PPO2 is low. PPO2's main innovation is to make the Kullback-Leibler penalty coefficient's theoretical procedure simpler. Its feature as a policy gradient approach is to directly train an unsupervised model or neural network during training.

Jobs coming from the southbound applications plane are scheduled by the control plane and sent to the SMP for performance.

When planned on the same kind of SMP resources, security enterprise background jobs run quickly; when scheduled on various types of resources, they run slowly. Table 1 displays the median processor ability of SMP capabilities to manage various task kinds [25].

Table 1 The average processing capacity of the middle platform assets for security [25]

	Computing-intensive job	*IOT-intensive job*
High-CPU Smp resources	AVG 1000MIPS STD 100	AVG 500MIPS STD 50
High-IOT Smp resources	AVG 500MIPS STD 100	AVG 5000MIPS STD 100

In addition, three different workload patterns were identified, with every workload's task time created at random following the same pattern. The parameters that make up the three repeated work patterns that make up the controlled setting can be found in Table 2 below. There were continuous modifications to the probability dispersion of the various types of professions all over time.

Table 2 Compilation of load modes.

Workload models	***Arrival Rate***	***Avg (%)***	***STD (%)***
Random	[0,100]	54.36	28.99
Low-frequency	[20,40]	39.65	9.68
High-frequency	[60,40]	69.56	49.96

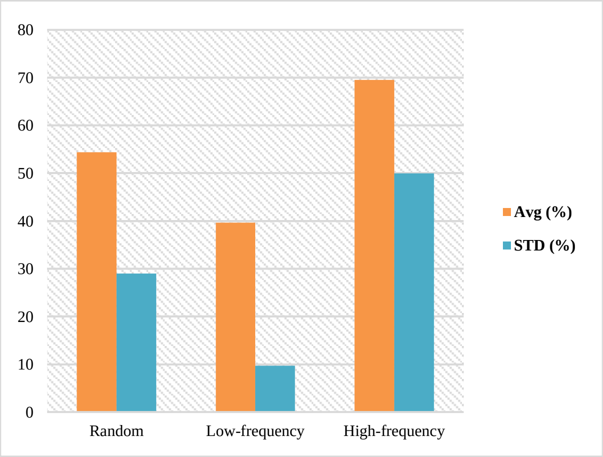


Fig. 3 Assembly of load modes.

When compared to the current approaches, the suggested approach can more cost-effectively schedule the front-end tasks to SMP resources and, following a brief learning curve, [26] enhance performance across all workload modes.

Table 3 The outcomes of the various workload modes in experiments [26]

Workload modes	*Metric*	*DQN*	*Random*	*RR*	*Earlist*	*Suitable*	*Sensibleif*
Random	**Cost**	323.59	391.25	362.69	385.23	359.59	349.69
	QoS Satisfaction	96.5%	54.5%	59.2%	49.8%	67.6%	97.9%
	Balancing rate	63.8%	79.6%	79.5%	79.5%	89.9%	56.9%
	Response time	0.985	0.497	0.216	0.589	0.549	0.259
Low-frequency	**Cost**	109.30	107.2	236.5	463.7	493.9	479.9
	QoS Satisfaction	99.9%	99.5%	98.6%	89.6%	97.6%	49.9%
	Balancing rate	26.9%	24.5%	47.9%	69.9%	75.6%	59.6%
	Response time	0.197	0.359	0.179	0.497	0.291	0.298
High-frequency	**Cost**	391.25	362.69	385.23	463.7	493.9	479.9
	QoS Satisfaction	99.9%	99.5%	98.6%	89.6%	97.6%	49.9%
	Balancing rate	26.9%	89.6%	97.6%	49.9%	75.6%	59.6%
	Response time	0.197	0.359	0.985	0.497	0.216	0.589

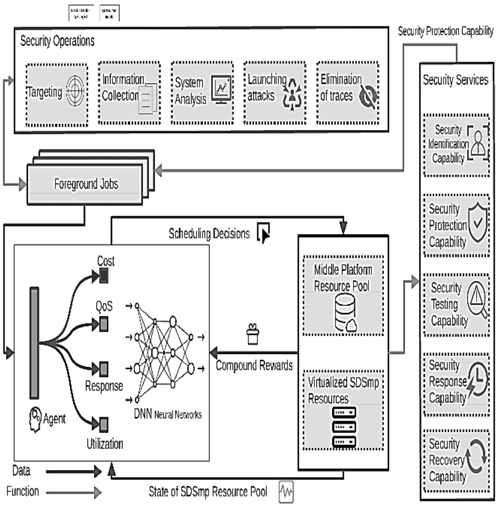
Table 3 displays the result for an aggregate of 2 hours in three duty modes: at random, low-frequency, and high-frequency, in addition to the initial 40 seconds. The offline education phase was interfering with the official functioning and real-time scheduling, thus the first forty seconds of instruction were eliminated.

$$Return = \sum_{t=0}^{n} R_t y_t \qquad \textbf{...8}$$

$$min_{\emptyset} \sum_{i=1}^{|B|} (r_{tr} + \gamma max\overset{\frown}{a\epsilon A}\, Q_{\emptyset}^{target}\, (st_i + 1, \hat{a}) - Q_{\emptyset}(st_i + 1, \hat{a}))^2 \qquad \textbf{...9}$$

3.5. Our Scheduling Based on DRL

Two various kinds of arrows are utilized, as seen in Figure 4, to denote the functions represented and the data transmitted. The major optimisation goal is the cost, which is indicated in red. The security operations of the privacy service plane are used by the SDSmp plane of control to schedule the foreground jobs.



Security Operations
Targeting
Information Collection
System Analysis
Launching attacks
Elimination of traces
Security Protection Capability
Security Services
Security Identification Capability
Security Protection Capability
Security Testing Capability
Security Response Capability
Security Recovery Capability
Foreground Jobs
Scheduling Decisions
Cost
QoS
Response
Utilization
Agent
DNN Neural Networks
Compound Rewards
Middle Platform Resource Pool
Virtualized SDSmp Resources
Data
Function
State of SDSmp Resource Pool

Fig. 4 A DRL-based algorithm for the MPC-SDSmp's real-time cost optimization [27]

An instance is chosen out of the Smp resource pool to complete the task and get the reward, in keeping with the rules [27]. The DNN might take a long time to train because of its large state space. This can be prevented by using an event-driven decision approach.

4. Results and Discussion

The reinforcement learning framework for DRL-IDS, as presented in this paper, has its foundation on stable (2.10.0), an enhanced way to implement a set of algorithms for reinforcement learning depending on the OpenAI baseline and depending on Tensor Flow (1.14.0), a from beginning to end artificial intelligence system. Using the OpenAI Gym (0.17.2) library to complete the reinforcement learning tailored environment, a freely available Neural Network (NN), creation platform, and the model's performance is evaluated using four metrics: precision, recall, accuracy, and F1 score. The test in issue is a hardware experiment in Ubuntu 18.04.

Table 4 Description of data set.

Attack type	***Quality***	***Attack type description***
Normal	1497981	Normal network traffic
NMRI	2978	Normal malicious response injection
CMRI	156970	Complex malicious response injection
MSCI	89	Malicious status command injection
MPCI	9547	Malicious parameter command injection
MFCI	897	Malicious function command injection
DoS	1497	Denial of service attack
Reconnaissance	9782	Attack

The hidden component of the multiple-layer recognizing network is subsequently employed as the shared central network for a value chain and advantageous connection in conjunction with the method of deep learning. The most compelling set of includes is extracted from the Industrial Network of Things data using the GBM's feature selection the system.

Model training is implemented in the experiment using the PPO2 interfaces of the Stable baseline [28]. Table 5 enumerates the primary training process parameters. Lastly, Table 3's learning and validation sets are used to evaluate the DRL-IDS detection agent. Table 5 presents the results, and every indication is greater than 97%.

Table 5 DRL-IDS classification report.([28]

Attack type	***F1 score***	***Recall***	***Precision***	***Accuracy***
Normal	0.9795	0.9879	0.9789	0.9648
NMRI	0.9750	0.9561	0.9456	0.9234
CMRI	0.9790	0.9236	0.9726	0.9634
MSCI	0.9760	0.9316	0.9761	0.9236
MPCI	0.9316	0.9631	0.9756	0.9316
MFCI	0.9791	0.9867	0.9641	0.9641
DoS	0.9864	0.9579	0.9726	0.9365
Reconnaissance	1,000,000	1,000,000	1,000,000	0.9909

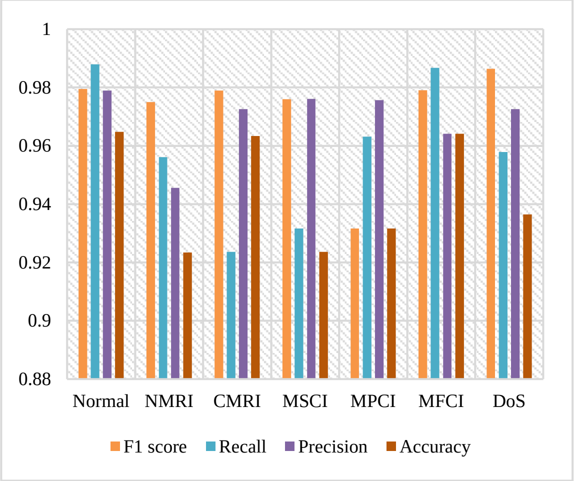


Fig. 5 DRL-IDS classification report [28].

Table 6 Matrix of Confusion.

	Recall	***Precision***	***F1 score***
Test	99.05	98.60	97.08
Train	99.7	98.69	97.97
Validate	95.62	98.59	97.08

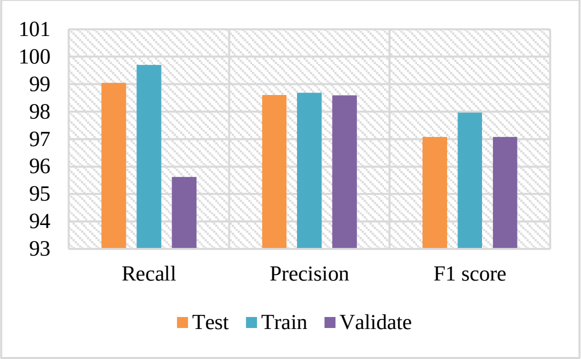


Fig. 6 Matrix of Confusion.

It demonstrates that every assault detection's recall rate, F1 score, and reliability are aimed at perfect. The comprehensive effectiveness of the assessment model is synthesized across all experiments using macro averages, and the DRL-IDS rate of accuracy is 99.09%.

This PPO2-based system for detecting intrusions is compared to another method, DDQN, in the context of reinforcement learning using an equivalent neural network structure. This document refers to the comparison algorithm's parameter parameters. In terms of degree, recall percentage, F1 score, and other metrics, it performs better compared to other benchmark systems.

Simultaneously, the comparison between the deeper learning-based detection technique and the deep reinforcement learning-based detection approach reveals that a reinforcement learning detection approach performs better overall depending on the depth. The simulation further compares the PPO2 algorithm-based detection system with the DRL-IDS presented in this study, according to in Table 7.

When dealing with the same volume of data, there are two types of intrusion detection systems: one based on DDQN and the other on DQN. The DQN-based intrusion detection system requires 18945 [29]. The findings indicate that the Industrial Internet of Things model based on PPO2 has an inexpensive cost of intrusion detection instruction of ten seconds, making it a better fit for real-world intrusion detecting scenarios.

Table 7 Comparing performance with alternative detection models.

	Accuracy	***Perception***	***Recall***	***F1 score***
CNN	0.9785	0.9648	0.9815	0.9648
RNNN	0.9531	0.9567	0.9648	0.9626
LSTM	0.9746	0.9647	0.9964	0.9731
DDQN	0.9641	0.9655	0.9640	0.9647
DQN	0.9764	0.9781	0.9360	0.9652

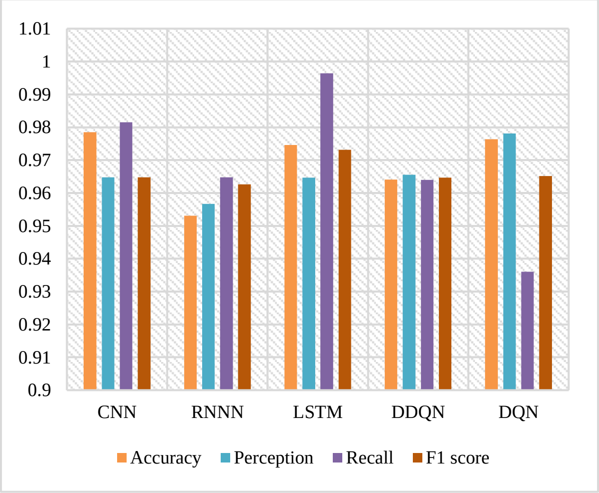


Fig. 7 Comparing performance with alternative detection models.

A. Prospects for Machine Learning-Powered IoT and Its Deployment Obstacles

It is anticipated that the vast majority of the applications pertaining to safe and intelligent driving will be entirely automated by 2030 in the context of self-driving automobiles. With the use of machine learning, deep learning, and other techniques, which are crucial to the growth of the majority of autonomous driving applications, the expectation will soon come true. The aforementioned methods can create algorithms that do intelligent learning and forecasts about administration of resources, management, and safety of networks [30]

Future technological developments will make networks of vehicles and the connections between computing, communication, and resource management increasingly intricate. To meet the increasing demands for quality of service, deep learning approaches have been the focus of most recent research. A few obstacles that create a rich setting for further study are encountered by researchers when attempting to apply machine learning processes to Internet of Things projects.

5. Conclusions

This article applies the PPO2 algorithm to construct a model for identifying an Industrial Network of Things. DRL-IDS utilizes LightGBM to efficiently extract a very attractive feature set from the data obtained from the Commercial Web of Things. This discussion pertains to the recent release of data on the Internet of Things (IoT) data collecting within the United States, specifically focusing on its relevance to the general population. The efficacy of the intrusion detection system, namely the Deep Reinforcement Learning-based Graphical Detection System (DRL GDS), in detecting different forms of network attacks within the context of the Industrial Internet of Things (IIoT) has been demonstrated through numerous experiments conducted at the Oak Ridge National Laboratory, a research facility under the U.S. Department of Energy. The proposed system exhibits superior performance compared to the currently employed deep learning- or deep reinforced learning-based intrusion detection systems, as measured by metrics such as recall, accuracy, precision, rate, and F1 score. The utilization of this technique significantly reduces the duration required for training intrusion detection models.

Future work

This research work in future research will examine extended distributed architecture-based industrial Internet of Things intrusion detection systems.

References

[1] Harika, J.; Baleeshwar, P.; Navya, K.; Shanmugasundaram, H. A review on artificial intelligence with deep human reasoning. In Proceedings of the 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 9–11 May 2022; pp. 81–84.

[2] Farhan, L.; Hameed, R.S.; Ahmed, A.S.; Fadel, A.H.; Gheth, W.; Alzubaidi, L.; Fadhel, M.A.; Al-Amidie, M. Energy efficiency for green internet of things (IoT) networks: A survey. Network 2021, 1, 279–314.

[3] Almusaylim, Z.A.; Zaman, N. A review on smart home present state and challenges: Linked to context-awareness internet of things (IoT). Wirel. Netw. 2019, 25, 3193–3204.

[4] Amin, F.; Abbasi, R.; Mateen, A.; Ali Abid, M.; Khan, S. A step toward next-generation advancements in the internet of things technologies. Sensors 2022, 22, 8072.

[5] Barnett, G.A.; Ruiz, J.B.; Xu, W.W.; Park, J.Y.; Park, H.W. The world is not flat: Evaluating the inequality in global information gatekeeping through website co-mentions. Technol. Forecast. Soc. Chang. 2017, 117, 38–45.

[6] Alhaj, A.N.; Dutta, N. Analysis of security attacks in SDN network: A comprehensive survey. In Contemporary Issues in Communication, Cloud and Big Data Analytics: Proceedings of CCB 2020; Springer: Singapore, 2022; pp. 27–37.

[7] Qiu, R.; Qin, Y.; Li, Y.; Zhou, X.; Fu, J.; Li, W.; Shi, J. A software-defined security middle platform architecture. In Proceedings of the 5th International Conference on Computer Science and Software Engineering, Guilin, China, 21–23 October 2022; pp. 647–651.

[8] W. Rafique, L. Qi, I. Yaqoob, M. Imran, R. U. Rasool, and W. Dou, “Complementing IoT services through software-defined networking and edge computing: a comprehensive survey,” IEEE Communications Surveys & Tutorials., vol. 22, no. 3, pp. 1761–1804, 2020.

[9] P. Sivakumar, “Improved Resource management and utilization based on a fog-cloud computing system with IoT incorporated with Classifier systems,” Microprocessors and Microsystems, 2021.

[10] S. Khan, M. Ali, N. Sher, Y. Asim, W. Naeem, and M. Kamran, “Software-defined networks (SDNs) and internet of things (IoTs): a qualitative prediction for 2020,” International Journal of Advanced Computer Science and Applications, vol. 7, no. 11, 2016.

[11] Restuccia, F., D’Oro, S., & Melodia, T. (2018). Securing the internet of things in the age of machine learning and software-defined networking. IEEE Internet of Things Journal, 5(6), 4829-4842.

[12] Dai, M., Su, Z., Li, R., & Yu, S. (2021). A Software-defined-networking-enabled approach for edge-cloud computing in the Internet of Things. IEEE Network, 35(5), 66-73.

[13] Bahashwan, A. A., Anbar, M., Manickam, S., Al-Amiedy, T. A., Aladaileh, M. A., & Hasbullah, I. H. (2023). A Systematic Literature Review on Machine Learning and Deep Learning Approaches for Detecting DDoS Attacks in Software-Defined Networking. Sensors, 23(9), 4441.

[14] Shukla, P. K., Maheshwary, P., Subramanian, E. K., Shilpa, V. J., & Varma, P. R. K. (2023). Traffic flow monitoring in software-defined network using modified recursive learning. Physical Communication, 57, 101997.

[15] Negera, W. G., Schwenker, F., Debelee, T. G., Melaku, H. M., & Feyisa, D. W. (2023). Lightweight Model for Botnet Attack Detection in Software Defined Network-Orchestrated IoT. Applied Sciences, 13(8), 4699.

[16] Wang, P., Yang, L. T., Nie, X., Ren, Z., Li, J., & Kuang, L. (2020). Data-driven software defined network attack detection: State-of-the-art and perspectives. Information Sciences, 513, 65-83.

[17] Assis, M. V., Carvalho, L. F., Lloret, J., & Proença Jr, M. L. (2021). A GRU deep learning system against attacks in software defined networks. Journal of Network and Computer Applications, 177, 102942.

[18] Mohammed, S. S., Hussain, R., Senko, O., Bimaganbetov, B., Lee, J., Hussain, F. ... & Bhuiyan, M. Z. A. (2018, October). A new machine learning-based collaborative DDoS mitigation mechanism in software-defined network. In 2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) (pp. 1-8). IEEE.

[19] Alajdah, A. H. I. (2022). A new software defined network (SDN) in IoTs based deep learning techniques (Master's thesis, Altınbaş Üniversitesi/Lisansüstü Eğitim Enstitüsü).

[20] Saqib, M., Khan, F. Z., Ahmed, M., & Mehmood, R. M. (2019). A critical review on security approaches to software-defined wireless sensor networking. International Journal of Distributed Sensor Networks, 15(12), 1550147719889906

[21] X. Li, L. Ji, H. Zhu, P. Li, X. Jia, and C. Li, “Cellular automata-based simulation of cross-space transmission of energy local area network risks: a case study of a power supply station in Beijing,” Sustainable Energy, Grids and Networks, vol. 27, Article ID 100521, 2021.

[22] L. Leenen and T. Meyer, “Artificial intelligence and big data analytics in support of cyber defines,” In Research Anthology on Artificial Intelligence Applications in Security 2021, IGI Global, pp. 1738–1753.

[23] T. P. Latchoumi and L. Parthiban, “Quasi oppositional dragonfly algorithm for load balancing in cloud computing environment,” 2021.

[24] Bicaku, M. Tauber, and J. Delsing, “Security standard compliance and continuous verification for industrial internet of things,” International Journal of Distributed Sensor Networks, vol. 16, no. 6, Article ID 155014772092273, 2020.

[25] Nižetić, P. Šolić, D. López-de-Ipiña González-de-Artaza, and L. Patrono, “Internet of Things (IoT): opportunities, issues and challenges towards a smart and sustainable future,” Journal of Cleaner Production, vol. 274, Article ID 122877, 2020.

[26] M. Razian, M. Fathian, and R. Buyya, “ARC: anomaly-aware Robust Cloud-integrated IoT service composition based on uncertainty in advertised quality of service values,” Journal of Systems and Software, vol. 164, Article ID 110557, 2020.

[27] W. T. Vambe, C. Chang, and K. Sibanda, “A review of quality of service in fog computing for the Internet of Things,” International Journal of Flow Control, vol. 3, no. 1, pp. 22–40, 2020.

[28] J. Ramakrishnan, M. S. Shabbir, N. M. Kassim, P. T. Nguyen, and D. Mavaluru, “A comprehensive and systematic review of the network virtualization techniques in the IoT,” International Journal of Communication Systems, vol. 33, no. 7, Article ID e4331, 2020.

[29] S. Zroug, I. Remadna, L. Kahloul, S. Benharzallah, and S. L. Terrissa, “Leveraging the power of machine learning for performance evaluation prediction in wireless sensor networks,” in Proceedings of the 2021 International Conference on Information Technology (ICIT), pp. 864–869, IEEE, Amman, Jordan, 2021 Jul 14.

[30] Y. Xiao, G. Niu, L. Xiao, Y. Ding, S. Liu, and Y. Fan, “Reinforcement learning based energy-efficient internet-of-things video transmission,” Intelligent and Converged Networks, vol. 1, no. 3, pp. 258–270, 2020.