This article has been accepted for publication in IEEE Transactions on Consumer Electronics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TCE.2024.3472071

Secure and Efficient AI-SDN-based Routing for Healthcare-Consumer Internet of Things

Zabeehullah, Nauman Ali Khan, Ikram Ud Din *Senior Member, IEEE*, Ahmad Almogren *Senior Member, IEEE*, Ayman Altameem, and Mohsen Guizani *Fellow, IEEE*

***Abstract*—The advancement of communication technologies and cloud systems has led to the emergence of the Healthcare-Consumer Internet of Things (H-CIoT) as a significant domain. This emergence has transformed the traditional healthcare system into the next generation of H-CIoT, characterized by higher connectivity and intelligence. Software-Defined Networking (SDN) is currently being incorporated into H-CIoT, enabling it to meet the complex, dynamic, and heterogeneous requirements of H-CIoT networks. As the H-CIoT network expands, there is an increasing demand for secure, efficient, and optimal routing to ensure low latency and high throughput. In this paper, we propose an Artificial Intelligence (AI)-based approach that combines the strengths of Generative Adversarial Networks (GANs) and Deep Reinforcement Learning (DRL) to accurately detect anomalies in H-CIoT imbalance data and achieve optimum routing. The DRL model dynamically formulates the optimal routing policies through efficient adaptation to underlying network traffic patterns. It also comprehends the characteristics of imbalance data to enhance its routing decisions. Simulation-based results validate the effectiveness and superiority of our proposed model over OSPF routing optimization technique in term of throughput (12%), latency (20%), and the Probability of avoiding malicious minor class attacks (30%), confirming it as an outstanding suitability for the next-generation H-CIoT network.**

***Index Terms*—Artificial Intelligence, Healthcare-Consumer Internet of Thing, Software Defined Network, Cloud Computing, Routing Optimization, Security.**

I. Introduction

THE emergence of the Internet of Things (IoT) in recent years is driving a fundamental transformation in various areas of human-machine interaction. The IoT focused on the consumer healthcare domain is known as Healthcare Consumer Internet of Things (H-CIoT). The H-CIoT marks a transition towards ubiquitous monitoring of the patients which aids in the early detection of disorders and the implementation of a proactive treatment plan [1], [2]. The H-CIoT is based on Body Sensor Network (BSN) technology which uses sensors around the human body. The most common use of H-CIoT at the moment is smart wearable fitness tracking [3], [4], [5].

Zabeehullah, and Nauman Ali Khan are with the Department of Computer Software Engineering, National University of Sciences and Technology (NUST), Islamabad, Pakistan. (email: zabeeh.phdcse@students.mcs.edu.pk, nauman.ali@mcs.nust.edu.pk); I. U. Din is with the Department of Information Technology, The University of Haripur, 22620 Haripur, Pakistan (e-mail: ikramuddin205@yahoo.com); A. Almogren and A. Altameem are with the Chair of Cyber Security, Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh 11633, Saudi Arabia (email: ahalmogren@ksu.edu.sa, aaltameem@ksu.edu.sa); M. Guizani is with the Mohamed bin Zayed University of Artificial Intelligence, Abu Dhabi, UAE (e-mail: mguizani@ieee.org).
Corresponding authors: Ahmad Almogren, Ikram Ud Din

The H-CIoT smart devices have a complex, heterogeneous, and dynamic nature. The conventional network infrastructure finds it difficult to adjust to the dynamic nature of H-CIoT applications and does not support H-CIoT architecture. Currently, Software-Defined Network (SDN) has emerged as a novel next-generation networking paradigm and manages H-CIoT infrastructure complexity, heterogeneity, and dynamicity efficiently. SDN uses OpenFlow protocol for communication between the data plane and the control plane. By using the OpenFlow protocol, the SDN controller discovers the network topology and selects the forwarding routes dynamically. The H-CIoT applications are latency-sensitive and time-critical which demand a high level of security and Quality of Service (QoS) in terms of routing optimization.

The associated challenges with the SDN-based H-CIoT are: 1) SDN default routing protocols such as OSPF and RIP are vulnerable to imbalance security attacks and threats. That indicates that most network flow data is from legitimate traffic, and malicious activity that could lead to a service outage only sometimes occurs. Furthermore, the majority of attacks fall under the category are well known, whereas certain types of attacks are incredibly rare. Moreover, because of software and hardware technological advancement, the attack surface has increased and it is very difficult to detect minor class attacks. These protocols work on the basis of shortest path routing policies and can not efficiently manage H-CIoT dynamic traffic flows and imbalance security attacks which result from system performance deterioration in terms of high latency, increased packet loss rate, and low throughput. 2) As the H-CIoT network expands, it is very important to fulfill the heterogeneous and critical requirements of the H-CIoT system. For this, efficient and intelligent routing is required to forward H-CIoT data to the required cloud system with minimum latency, high bandwidth, and security. To handle security and QoS problems simultaneously is usually a challenging task.

To tackle the above-mentioned challenges, this article concentrates on secure and optimized routing within SDN-based H-CIoT systems to fulfill QoS demands. The proposed model integrates two Artificial Intelligence (AI) models: Generative Adversarial Network (GAN) and Deep Reinforcement Learning (DRL). To the best of our knowledge, this article represents the first endeavor to accomplish both secure and optimized routing in H-CIoT. The main contributions of this article are outlined below:

- We propose an SDN and GAN-DRL intelligent model to achieve secure and optimized routing within the H-CIoT environment.

Authorized licensed use limited to: VIT-Amaravathi campus. Downloaded on July 29,2025 at 05:55:58 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Consumer Electronics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TCE.2024.3472071

- The GAN model accurately identifies imbalance data security attacks by generating plausible synthetic data. Subsequently, DRL optimizes routing by interacting with the underlying environment and updating parameters based on achieving maximum cumulative rewards.
- We conducted a performance analysis of the proposed model in contrast to the baseline routing algorithm, namely Open Shortest Path First (OSPF), to thoroughly evaluate the proposed approach. To ensure a fair comparison, both models underwent training and assessment within same environments.

The remainder of this article is structured as follows: Section II provides a concise overview of related work. Section III outlines the problem and imbalance attacks. Section IV presents the proposed model scheme. Section V details the experimental setup and evaluation metrics. Section VI discusses the attained results. Finally, conclusion is drawn in Section VII.

II. Related Work

A. SDN and Healthcare Consumer IoT

In this subsection, we will examine the literature on SDN and Healthcare Consumer IoT. How the SDN can help with the complexity, heterogeneity, security, and routing optimization issues associated with the Healthcare Consumer IoT or Internet of Medical Things (IoMT). The authors of [6] provide the detailed review of Healthcare 5.0 and its integration with state-of-the-art technologies like SDN, edge, and cloud based computing. This article [7] proposed an SDN model for IoMT devices to address the imbalance data security challenge.

Babbar *et al.* [8] proposed a SDN-based security compliance framework for smart healthcare load migration systems in order to address security attack challenges. The proposed framework and algorithm provide 80% accuracy for all healthcare data packets retrieved, enabling secure data management. Sarkar *et al.* [9] proposed an Intelligent Software-defined Fog Architecture (i-Health) framework. The controller will determine whether to send the data to the fog layer based on each patient's historical data pattern. This study presents a novel method that clusters patients with e-health IoT devices based on similarity and distance using a spectral clustering technique [10]. The vast processing capacity of a GPU is utilized in [11] to present a SDN based on an analytical parallel routing architecture for dynamically optimizing multiconstrained QoS parameters in the IIoT. Using SDN controller, the author of [12] proposed a secure, energy-conscious routing system that allows different IoT devices with constrained energy and resource availability to communicate with one another.

B. AI for SDN based Healthcare Consumer IoT

The authors of [13] present a novel method for improving cloud security based on consumer IoT and using AML approaches in smart healthcare. In [14], the authors proposed an SDN-enabled IoMT healthcare network, a novel Medical Traffic Forecasting framework based on Weighted Multivariate Singular Spectrum Analysis (MTF-WMSSA) is presented to anticipate and analyze network traffic and guarantee accurate real-time medical data transfer. The authors of [15] addressed different security concerns and used onion routing to resolve them. In [16], the authors devised an SDN-based design for complicated and heterogeneous IoMT networks. The work in [17] presents a cross-architecture IoMT malware detection and classification system based on byte sequences retrieved from Executable and Linkable Format. Using characteristics of network flows and patient biometrics, the study [18] proposes a deep learning-based method for network-based intrusion detection in Internet of medical things (IoMT) systems. To address the routing problem, the authors of this study [19] provide a new modeling paradigm structured around a two-level control mechanism. A deep-learning-based image encryption and decryption network (DeepEDN) is presented in [20] to complete the encryption and decryption of the medical image. In their paper [21], the authors introduced a novel deep reinforcement learning (DRL) framework dubbed DQQS, designed to optimize Quality of Service (QoS) and Quality of Experience (QoE) while safeguarding the security of SDN-IoT networks.

III. Problem Description

Within this section, we commence by introducing the network structure and defining the problem, followed by an overview of the attack model. The notations utilized throughout this paper are consolidated in Table I.

TABLE I
SYMBOLS USED IN NETWORK MODEL

Symbols	Explanation
$\mathbb{S}$	Represents the number of SDN-enabled switches
$\mathbb{L}$	Represents the links between SDN-enabled switches
$\mathbb{F}_{s_i}$	Represents maximum flows in any switch $s_i, i = 1, 2, 3...$
$\mathbb{F}_{s_i}(t)$	Represent how many flow entries can be accommodated by switch s_i at any time t
$\mathbb{R}_{p(s_s,s_d)}$	Routing policy request from source switch s_s to the destination switch s_d
s_s	Represent the source switch
s_d	Represent the destination switch
$\mathbb{RS}$	Set of relay switch
$\mathbb{N}(\mathbb{S},\mathbb{L})$	Network with $\mathbb{S}$ number of SDN-enabled switches and $\mathbb{L}$ links between switches

A. Problem and H-CIoT Networking Structure

To enhance clarity and comprehension of the data plane's packet forwarding process within the SDN-based H-CIoT environment, important terms and definitions are provided in Table I. Here, $\mathbb{N}(\mathbb{S},\mathbb{L})$ denotes the network configuration comprising $\mathbb{S}$ SDN-enabled switches and $\mathbb{L}$ undirected links connecting these switches. In the SDN-based H-CIoT network environment, each SDN-enabled switch, represented as s_i, is equipped with a flow table, and network control and management are centralized under the SDN controller $\mathbb{C}$. The SDN controller possesses the capability to deploy a flow entry based on the H-CIoT environmental requirements. Fig. 1 shows the packet forwarding procedure of the proposed model. The

Authorized licensed use limited to: VIT-Amaravathi campus. Downloaded on July 29,2025 at 05:55:58 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Consumer Electronics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TCE.2024.3472071

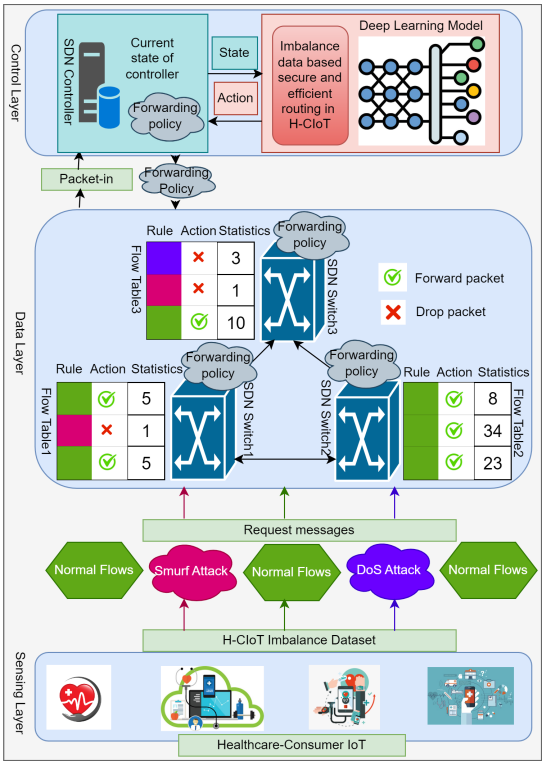

Fig. 1. The workflow of the SDN based deep learning proposed model to tackle H-CIoT imbalance security attacks to achieve optimized routing.

imbalance data is gathered by the H-CIoT sensing layer and forward to the upper layer (data layer). The SDN-based switch then searches the flow database for a flow entry that matches. The flow table directs the forwarding process if such an entry is present. A packet-in message is sent to the controller if not. The controller decides what to do after receiving the packet-in message and sends out a forwarding policy to update the flow table in the switch that has enabled OpenFlow. In the event that a data layer small-scale class attack occurs during this procedure, the OSPF routing protocol is usually left vulnerable and is unable to recognize the effect of the imbalance data minor class attacks. As such, this situation is likely to result in increased latency, reduced network performance, and network data congestion.

SDN and AI offer a promising avenue for tackling the challenges of imbalance data security and intelligent routing optimization in H-CIoT. Thus, in our proposed SDN-based GAN-DRL model, the SDN controller has evolved to possess the intelligence required to accurately identify and detect minor class attacks on H-CIoT imbalance data, enabling optimized routing.

IV. The Proposed Model Scheme

This section goes over the proposed model's architecture. Fig. 2 displays the architecture of the proposed model.

The core element of the proposed AI-SDN based H-CIoT paradigm is the control layer, which communicates with the cloud layer via the northbound interface and the data plane through the southbound interface. In order to identify and

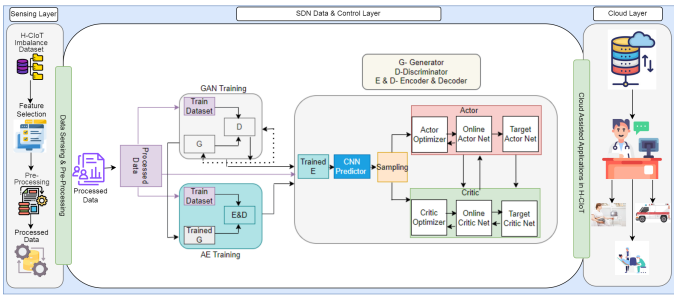

Fig. 2. The proposed efficient and secure routing model for H-CIoT.

mitigate H-CIoT imbalance data security threats and perform routing optimization, we have integrated GAN-DRL deep learning models into SDN controller.

A. Architecture of GAN Model

1) Synthetic Data Generation: The synthetic data generation is used to build and train the generative model using the refined dataset. Boundary Equilibrium Generative Adversarial Network (BEGAN) is the generative model we used, and it performs similarly to the AE. We built the generator as a symmetric five-layer AE model, utilizing the same architecture as the discriminator's decoder. The system creates generative models for each divided sub-data set after first classifying the given data set. The BEGAN model is then trained using these models. Stated differently, generative models are constructed in an equal number of classes and they only offer synthetic data corresponding to individual classes once they have been trained. To use the BEGAN model for minor class anomaly detection, it is important to establish the criterion for ending the training process. Because it directly affects the synthetic data that is used to train the detection model, this choice has a big effect on how effective anomaly detection is. The ability of BEGAN to estimate training convergence using the equilibrium concept distinguishes it from other GAN models.

The convergence measure (M) is used to terminate the training phase of a generative model. Throughout training, the system input parameter is regarded as a threshold value, and the training process ends if the convergence measure (M) drops below the specified threshold. We set the (M) threshold value at 0.058 in our proposed paradigm.

2) AE Training: To create a useful imbalance data anomaly detection model, the AE model is first trained to perform dimension reduction and feature extraction operations. Our proposed model's AE architecture and the discriminator's design from the generative model are identical. The expanded dataset is used to build an AE model, which is then trained before the trained encoder is used in the feature extraction procedure. Notably, the trained encoder is positioned first in the input layer of the detection models. It is configured to function solely as a feature extractor, with no further learning during the training of detection models.

3) Predictive Model Training: At this stage, we classified anomalies using a Convolutional Neural Network (CNN). For the purpose of classifying the H-CIoT imbalance dataset,

Authorized licensed use limited to: VIT-Amaravathi campus. Downloaded on July 29,2025 at 05:55:58 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Consumer Electronics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TCE.2024.3472071

one-dimensional (1-D) convolutional layers are used in the construction of the CNN rather than converting the input data into two-dimensional space. As a result, two one-dimensional convolutional layers and one fully linked layer make up the CNN model. Algorithm 1 presents the whole procedure for training the predictive model using the trained generators and encoder.

Algorithm 1 Classifier Training

INPUT : Training DataSet (TD) TD_{train}, set of generators $\mathbf{G}$, and Trained Encoder (μ_E)
OUTPUT: Trained Classifier (χ_{μ_E})
Initialization of classifier parameters χ^0
for $G_i \in \mathbf{G}$, where $1 \leq i \leq k$ do
$\mathbf{z} = \{z_j\} j = 1, 2, 3...., m_i$
Synthetic DataSet (SD) = $G_i(\mathbf{z})$
end for
Expanded Dataset (ED) = $TD_{train} \cup SD_1 \cup ..... \cup SD_k$
Trainable state of μ_E is set to false
Build $\chi^0_{\mu_E}$ = Model-Concatenation (μ_{AE}, χ^0)
χ_{μ_E} = Train-Classifier $(\chi^0_{\mu_E}, ED)$

B. Architecture of DRL

1) State: We consider the routing in H-CIoT is taking place within a unit of time, with each unit equivalent to one time step. Consequently, the total routing time between the source switch s_s and the destination switch s_d is denoted as $\mathbb{T}$. In a single unit time slot, the DRL agent assesses the reward for a transmission task that consists of timing how long it takes to choose the next SDN-enabled hop switch and send data to it. The flow table's message holding rate, $\rho_s(t)$; the channel holding rate between the SDN controller and the switch, $\sigma_s(t)$, and message input frequency, $\lambda_s(t)$, are the three factors that the DRL agent uses to calculate the reward. When $t, t = (1, 2, 3, ...)$ is the unit time for a certain switch node $s_i, i = (1, 2, 3, ...)$, these three variables taken together determine the system's real state. Upon incorporating these three factors:

$$\begin{aligned} s(t) =& [\lambda_{s_1}(t), \lambda_{s_2}(t), \lambda_{s_3}(t), ...\lambda_{s_N}(t), \\ & \rho_{s_1}(t), \rho_{s_2}(t), \rho_{s_3}(t), ...\rho_{s_N}(t). \end{aligned} \tag{1}$$

2) Action: Smart and intelligent routing relies heavily on the selection of the next hop (switch). In the action stage, the primary responsibility of the DRL agent is to identify and choose the next available switch for data transfer. This action stage is depicted by Equation (3).

$$\mathbb{P}(t) = \mathbb{P}^{prest}_{s_1}(t), \mathbb{P}^{prest}_{s_2}(t), \mathbb{P}^{prest}_{s_3}(t), ...\mathbb{P}^{prest}_{s_N}(t). \tag{2}$$

As shown in a Equation (3), $\mathbb{P}^{prest}_{s_i}(t)$ can be defined in the vector form $\mathbb{P}^{prest}_{s_i}(t) = \{\mathbb{P}^{prest}_{s_i,s_j}(t) | J \in \{1, 2, 3...N\}, J \neq I\}$. $\mathbb{P}^{prest}_{s_i,s_j}(t)$ shows the relation between the switch s_i and the switch s_j. Every element of $\mathbb{P}^{prest}_{s_i,s_j}(t) \in [0, 1]$, where $\mathbb{P}^{prest}_{s_i,s_j}(t) = 0$ means there is no connection between switch s_i and switch s_j at any unit time t and $\mathbb{P}^{prest}_{s_i,s_j}(t) \in [0, 1]$ shows the switch s_j weight that which is selected as next hop of switch s_i.

3) Reward: In DRL, the efficiency and effectiveness of the agent's actions are assessed through the reward function. Consequently, the reward associated with each action varies. Within our proposed technique, key parameters defining the reward function include switch processing delay, switch forwarding delay, switch queuing delay, switch packet loss rate, and flow table status. QoS related parameters impacting the reward function encompass throughput, link packet loss rate, and latency. The reward function is articulated in Equation (5).

$$Attack(t) = \alpha RW^{attack(s \dashrightarrow d)}_{H-CIoT_i}(t), \tag{3}$$

$$RW(t) = \frac{1}{|Trans|} \sum_{i \in Trans} Attack(t) + \beta RW^{QoS}_{s_i}(t) \tag{4}$$

$$\begin{aligned} RW^{attack(s \dashrightarrow d)}_{H-CIoT_i}(t) =& - DEL^{process}_{s_i} - DEL^{queue}_{s_i} \\ & - DEL^{forward}_{s_i} - PLR_{s_i} + FTS_{s_i}. \end{aligned} \tag{5}$$

Now, QoS rewards are defined in Equation (7).

$$\begin{aligned} RW^{QoS}_{s_i}(t) = & \sum_{j \in \{1,2,3,4...N\}, j \neq i} (P^{prest}_{s_i,s_j}(t)(-DEL^{propagate}_{s_i,s_j} \\ & - Latency_{s_i,s_j})). \end{aligned} \tag{6}$$

C. Integration of the Proposed Technique with DDPG

1) DDPG: One of the most used DRL methods is DDPG [22]. The control layer of our proposed model utilizes DDPG as shown in a Fig. 2. It utilizes the DRL actor-critic paradigm, in which the actor consists of the actor network and the target actor network, represented by $\tau^{'}$ and $\tau(s|\theta^{\tau})$, respectively. In the same way, the critic consists of $\eta(s, a)$ and $\eta^{'}$, the target and primary critic networks, respectively. Both the target network and the main network have the same structure.. The current policy is determined by the actor-network $\tau(s|\theta^{\tau})$, which maps states to actions. The critic network $\eta(s, a)$ uses the Bellman equation as a learning tool, and the actor's output is usually used as the critic's input.

2) Sample Collection: Samples are created from the environment using the exploration policy, and sample records $(s(t), a(t), r(t), s(t + 1))$ are kept in a replay buffer B via the DDPG method. In this case, $s(t)$ and $a(t)$ stand for the starting state and output of the policy network, respectively. Furthermore, the state $s(t)$ is subjected to the action $a(t)$, which yields the associated rewards $r(t)$ and the ensuing state $s(t + 1)$.

3) Training: The training process is represented in an Equation (8)

$$Train(\theta) = \frac{1}{M} \sum_{t} (y(t) - \eta(s(t), a(t)|\theta^{\eta}))^2. \tag{7}$$

Authorized licensed use limited to: VIT-Amaravathi campus. Downloaded on July 29,2025 at 05:55:58 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Consumer Electronics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TCE.2024.3472071

Algorithm 2 Proposed Model Training

```
for epic = 1 to Trans do
    for t=1 to T do
        Transition from buffer B
        The training process is represented in an Equation (8)
        Target Q-value y(t) is defined in Equation (10)
        Parameters updation process is explained in Equation (12)
        Updating the target network by using Equation (13) and Equation (14)
    END
END
```

$$\eta(s(t),a(t)) \longleftarrow \eta(s(t),a(t)) + \zeta(r(s(t),a(t))) + \omega_{a(t+1)}\eta(s(t+1),a(t+1)) - \eta(s(t),a(t)). \quad (8)$$

In Equation (8), target Q-value $y(t)$ is defined as follow:

$$y(t) = r(t) + \omega\eta^{'}(s(t+1),\tau^{'}(s(t+1)|\theta^{\tau^{'}})|\theta^{\eta^{'}}). \quad (9)$$

By using the policy gradient technique, the gradient of the actor-network is given as:

$$\frac{\delta J(\theta^{\tau})}{\delta\theta^{\tau}} = Z_s[\frac{\delta\eta(s,a|\theta^{\eta})}{\delta a}\frac{\delta\tau^{'(s|\theta^{\tau})}}{\delta\theta^{\tau}}]. \quad (10)$$

Parameters updation process is explained in Equation (12)

$$\bigtriangledown_{\theta^{\tau}} J \approx \frac{1}{M}\sum_t \bigtriangledown_a \eta(s,a|\theta^{\eta})|_{s=s(t),a=\tau(s(t))} \bigtriangledown_{\theta^{\tau}} \tau(s|\theta^{\tau})|_{s(t)}. \quad (11)$$

Against the same state $s(t)$, main actor provides multiple actions. Hence, different actions can be used as an input for main critic to achieve different Q values. Equation (13) and Equation (14) update the target network

$$\theta^{\eta^{'}} \longleftarrow \phi\theta^{\eta} + (1-\phi)\theta^{\eta^{'}}, \quad (12)$$

$$\theta^{\tau^{'}} \longleftarrow \phi\theta^{\tau} + (1-\phi)\theta^{\tau^{'}}. \quad (13)$$

The detailed training mechanism of the proposed technique is elaborated in Algorithm 2.

D. Cloud Layer

In this layer, medical experts analyze the received dataset and take the necessary and appropriate actions.

V. EXPERIMENTAL SETUP AND EVALUATION METRICS

A. Experimental Protocol

We established the SDN-based H-CIoT environment using the Mininet 2.3.0 simulation tool. Subsequently, we deployed a Deep Learning model within the ONOS SDN controller, utilizing the Python-based TensorFlow framework. Our environment is equipped with the latest version of TensorFlow, v2.12.0. The simulations are carried out on a laptop with an 8th-generation Intel Core i9 processor, 16 GB of RAM, and a 1TB hard disk.

TABLE II
SDN-BASED H-CIOT IMBALANCE DATASET DISTRIBUTION

Class	Training	Weight%	Testing	Weight%
Normal	33,637	83 %	13,894	80%
DoS Attack	4,458	11%	1,476	8.5%
ARP Spoofing	1,366	3.37 %	1,077	6.2%
Nmap PortScan	851	2.1 %	677	3.9%
Smurf Attack	215	0.53 %	243	1.4%
Total	**40,527**	**100%**	**17,368**	**100%**

B. Hyperparameter Tuning

Three layers make up the GAN discriminator's design in the suggested methodology. There are 80 neurons in the first hidden layer, and there are 50 latent space dimensions. As a result, there are 80 neurons with a 50-dimensional latent space in the generator's hidden layer. ReLU is the activation function that is being used. Notably, the architecture of the AE is similar to that of the discriminator and it serves as a feature extractor. Additionally, we determined that 0.058 [23] is the GAN convergence threshold. If it drops below this threshold or reaches 280 epochs, the model's training phase comes to an end. Similarly, 300 epochs is the end of the AE training. We have chosen CNN with two hidden layers configured for classification. CNN uses a two-convolutional-layer, 1-D-CNN architecture. 32 convolutional filters make up the first layer, while 16 neurons make up the second, which is a fully connected layer. In the CNN, ReLU serves as the activation function. The DRL training network is constructed as a two-layer convolutional neural network (CNN), with relu serving as the first layer's activation function and tanh as the second. We use a random number of attack nodes to train the DDPG agent, and the simulation has 300 episodes.We update the network after calculating the cumulative prizes in each episode, with a maximum step of 20.

C. Dataset Description

The SDN-based H-CIoT dataset is highly imbalance, with three out of five classes (ARP Spoofing, Nmap PortScan, Smurf Attack) comprising less than 10% of the overall training data. With a weight of 0.53%, the Smurf Attack class has the lowest weight. This imbalance has a major effect on how the proposed model is trained. Additionally, simulations are performed in an SDN-based environment during the dataset's creation process.

As part of our methodology, we divided the dataset into training and testing sets, allocating 70% for training and 30% for testing purposes. The distribution of the dataset is detailed in Table II.

D. Evaluation Metrics

The proposed model is evaluated using three key metrics: throughput, latency, and the probability of avoiding the minor class attacks.

Authorized licensed use limited to: VIT-Amaravathi campus. Downloaded on July 29,2025 at 05:55:58 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Consumer Electronics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TCE.2024.3472071

VI. Result Analysis

The performance of the proposed model is assessed and compared with the OSPF routing protocol in this scientific work using the three common network metrics: throughput, latency, and the probability of avoiding minor class attacks. The rationale behind the comparison of the proposed model with OSPF is the extensive and rigorous evaluation and to show the effectiveness of the proposed technique. These measurements are critical for assessing the H-CIoT network, particularly when taking into account the effects of extremely minor class attacks such as the Smurf attack, which accounts for 0.53% of the total weight in the H-CIoT imbalance dataset.

First, the network metric throughput against both normal traffic and imbalance H-CIoT traffic—which includes extremely minor class attacks is used to assess and compare the performance of the proposed model with the OSPF. The comparison results of throughput for the two routing protocols against the normal traffic and imbalance traffic are given in Fig. 3 and Fig. 4, respectively. The findings presented in Fig. 3 demonstrate that both protocols exhibit high throughput values when compared to the normal traffic of the H-CIoT network. We can examine the effects of extreme minor class attacks on the throughput of both routing protocols in Fig. 4. In this instance, α and β, the reward parameters, are both set at 0.5. Under the extreme minor class Smurf attack, we can observe that the throughput of the proposed model increases by around 15% when compared to the throughput of OSPF. In comparison to the OSPF, the proposed model's throughput experiences a modest boost under the less minor class DoS attack.

The proposed model's superior performance over the conventional routing protocol, OSPF, against extreme minor classes attacks can be attributed to its GAN-DRL-based approach, which generates plausible synthetic data for minor classes and uses that information to accurately identify minor class attacks. After that, it chooses a secure routing path and decides more intelligently than OSPF. By classifying the attack category that the data belonged to, our proposed methodology creates synthetic data with varying levels of severity according to population weights. On our system, we generated synthetic data for minor classes with less than 10% weight in the distribution. In other words, we used the trained generative model to produce 5,000 synthetic data for each of the ARP Spoofing, Nmap PortScan, and Smurf classes. It is noteworthy that no extra synthetic data produced for the major classes. Furthermore, the classes with a weight of less than 1% are extremely minor classes such as Smurf attack. As with the experiments on the H-CIoT imbalance dataset, we used the original training and testing datasets (70% and 30% respectively). The evaluation of the proposed model is conducted on the original testing data set. In Fig. 5, the comparisons of the proposed model under different values of reward parameters are presented. It is evident that various reward parameters typically result in varying throughput numbers.

Secondly, we observed the performance of both protocols on the latency network metric. From the experimentation, it is clear that the latency of the proposed model is similar to OSPF under the attack-free H-CIoT environment. However, Fig. 6 shows that the latency of both protocols dramatically dropped to the lowest values under the extreme minor class Smurf attack. Still, the latency of the proposed model is relatively stable and lower than OSPF. This is because the proposed model efficiently detects and avoids minor class malicious attacks by perceiving the underlying environment. Furthermore, it is shown that the effects of various attacks on latency vary. The latency under various reward parameters is shown in Fig. 7. We can observe from the results that when α and β are 0.4 and 0.6, there is a slight increase in latency under the DoS attack. When α = 0.6, β = 0.4 are used as the reward parameters, the latency under the Smurf assault is slightly higher.

Thirdly, we noted the probability of both protocols in the H-CIoT context avoiding malicious minor class attacks. Based on the findings displayed in Fig. 8, the proposed model has a substantially higher probability of preventing malicious extreme minor class attacks than OSPF. By identifying minor class attacks, the proposed model ensures network QoS and increases the probability of achieving secure routing. The parameters used in the proposed model are given in Table III. Finally, comparison of the proposed model with state-of-the-art secure routing techniques exist in literature is given in Table IV.

TABLE III
List of parameters used in the proposed GAN-DRL model

Parameters	Value
ω	0.8
ζ	0.2
ϕ	0.03
(α, β)	(.5,.5),(.4,.6),,(.6,.4)

TABLE IV
Comparison of proposed model with advanced techniques

Ref.	Year	DL/SDN	Imbalance Security	Routing
[2]	2023	MFRLP	No	Yes
[3]	2023	AML-IDS	Yes	No
[7]	2024	GAN	Yes	No
[8]	2022	SDN-IIoT	Yes	No
[11]	2020	SDN-IIoT	No	Yes
Proposed Model	2024	GAN, DRL	Yes	Yes

VII. Conclusion

To provide efficient and secure routing in healthcare consumer IoT, we proposed an intelligent system based on deep learning and SDN. To manage the H-CIoT network's complexity, heterogeneity, distributed nature, and unexpected traffic flows, SDN is specifically integrated with it. Then deep learning model based on GAN and DRL is proposed to detect minor class attacks from H-CIoT imbalance data and perform intelligent routing. We demonstrated the effectiveness of the proposed paradigm in terms of throughput, latency, the probability of avoiding the minor class attacks and, speed efficiency through experimental evaluation on the SDN-based H-CIoT

Authorized licensed use limited to: VIT-Amaravathi campus. Downloaded on July 29,2025 at 05:55:58 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Consumer Electronics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TCE.2024.3472071

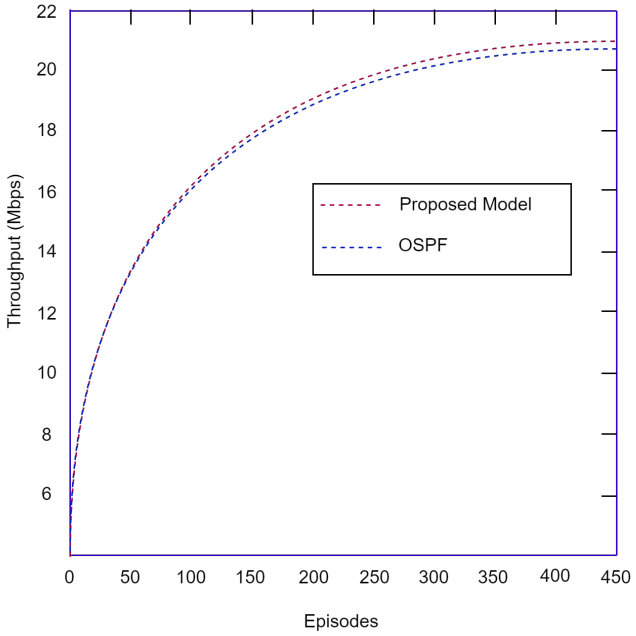

Fig. 3. Throughput of proposed model vs. OSPF in non-attacked H-CIoT network.

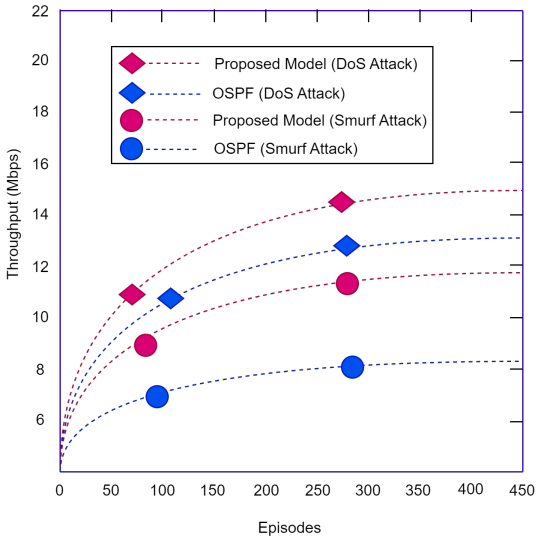

Fig. 4. Throughput of proposed model vs. OSPF in attacked H-CIoT network.

imbalance dataset. We also compared the performance of the proposed model against well known routing protocol, i.e., OSPF. To further enhance secure routing in these networks, we plan to integrate blockchain technology with the proposed technique to create a more robust, efficient, and secure model. Moreover, we also plan to test and validate the technique by training the model on various imbalanced datasets in future work.

ACKNOWLEDGMENT

This work was supported by the Deanship of Scientific Research at King Saud University, Riyadh, Saudi Arabia through the Vice Deanship of Scientific Research Chairs: Chair of Cyber Security.

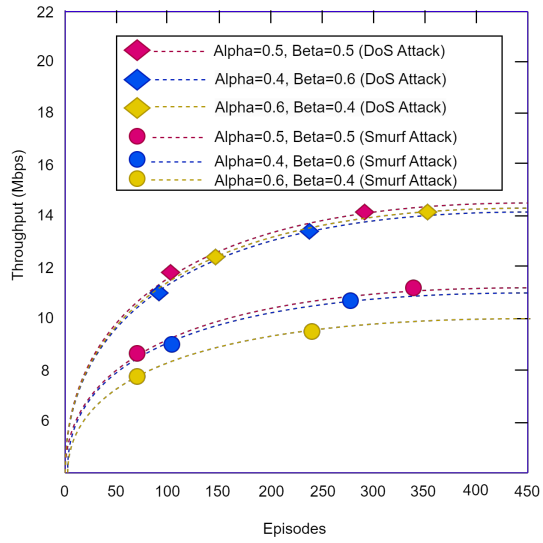

Fig. 5. Throughput of proposed model in attacked H-CIoT network with various parameters.

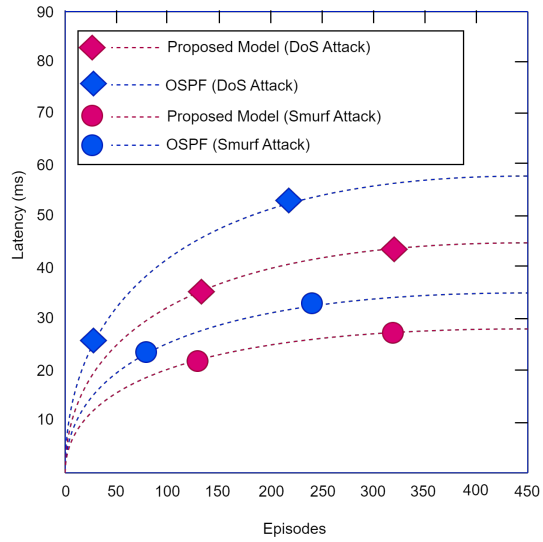

Fig. 6. Latency of proposed model vs. OSPF in attacked H-CIoT network.

REFERENCES

[1] S. Baker and W. Xiang, "Artificial Intelligence of Things for Smarter Healthcare: A Survey of Advancements, Challenges, and Opportunities," in IEEE Communications Surveys & Tutorials, vol. 25, no. 2, pp. 1261-1293, Mar. 2023.

[2] P. Tiwari, A. Lakhan, R. H. Jhaveri and T. -M. Grønli, "Consumer-Centric Internet of Medical Things for Cyborg Applications Based on Federated Reinforcement Learning," in IEEE Transactions on Consumer Electronics, vol. 69, no. 4, pp. 756-764, Nov. 2023.

[3] J. K. Samriya, C. Chakraborty, A. Sharma, M. Kumar and S. K. Ramakuri, "Adversarial ML-Based Secured Cloud Architecture for Consumer Internet of Things of Smart Healthcare," in IEEE Transactions on Consumer Electronics, vol. 70, no. 1, pp. 2058-2065, Feb. 2024.

Authorized licensed use limited to: VIT-Amaravathi campus. Downloaded on July 29,2025 at 05:55:58 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Consumer Electronics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TCE.2024.3472071

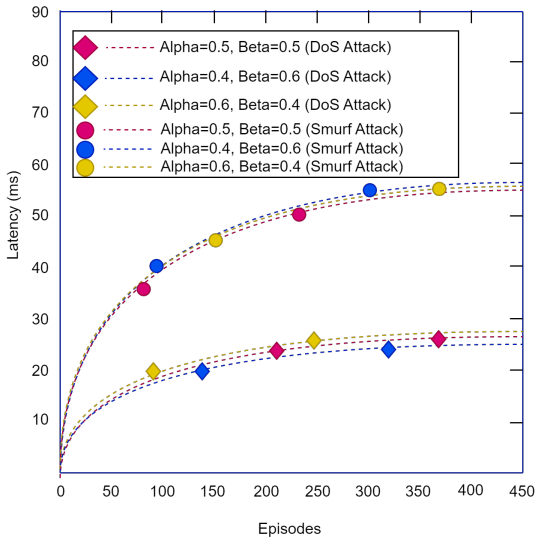

Fig. 7. Latency of proposed model in attacked H-CIoT network with various parameters.

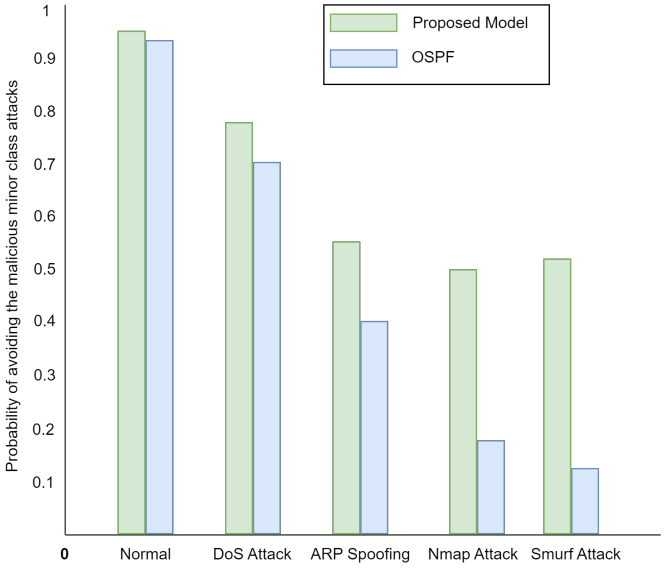

Fig. 8. Probability of avoiding malicious minor class attacks: Proposed model vs. OSPF.

[4] J. -H. Syu, J. C. -W. Lin, G. Srivastava and K. Yu, "A Comprehensive Survey on Artificial Intelligence Empowered Edge Computing on Consumer Electronics," in IEEE Transactions on Consumer Electronics, vol. 69, no. 4, pp. 1023-1034, Nov. 2023.

[5] Grows, Global Wearables Market. "7.7% in 4Q17 and 10.3% in 2017 as Apple Seizes the Leader Position, Says IDC." IDC: The premier global market intelligence company [Internet].[cited 10 Aug 2018]. Available: https://www. idc. com/getdoc. jsp (2018).

[6] H. R. Chi, M. de Fátima Domingues, H. Zhu, C. Li, K. Kojima and A. Radwan, "Healthcare 5.0: In the Perspective of Consumer Internet-of-Things-Based Fog/Cloud Computing," in IEEE Transactions on Consumer Electronics, vol. 69, no. 4, pp. 745-755, Nov. 2023.

[7] Zabeehullah, F. Arif, N. A. Khan, Q. Mazhar ul Haq, M. Asim and S. Ahmad, "An SDN-AI-Based Approach for Detecting Anomalies in Imbalance Data within a Network of Smart Medical Devices," in IEEE Consumer Electronics Magazine, doi: 10.1109/MCE.2024.3389292.

[8] H. Babbar, S. Rani and S. A. AlQahtani, "Intelligent Edge Load Migration in SDN-IIoT for Smart Healthcare," in IEEE Transactions on Industrial Informatics, vol. 18, no. 11, pp. 8058-8064, Nov. 2022.

[9] J.L. Sarkar, V. Ramasamy, A. Majumder, B. Pati, C.R. Panigrahi, W. Wang, N.M.F. Qureshi, C. Su, and K. Dev, "I-Health: SDN-Based Fog Architecture for IIoT Applications in Healthcare," in IEEE/ACM Transactions on Computational Biology and Bioinformatics, doi: 10.1109/TCBB.2022.3193918.

[10] Jazaeri, S.S., Asghari, P., Jabbehdari, S. et al. Composition of caching and classification in edge computing based on quality optimization for SDN-based IoT healthcare solutions. J Supercomput 79, 17619–17669 (2023).

[11] F. Naeem, M. Tariq and H. V. Poor, "SDN-Enabled Energy-Efficient Routing Optimization Framework for Industrial Internet of Things," in IEEE Transactions on Industrial Informatics, vol. 17, no. 8, pp. 5660-5667, Aug. 2021.

[12] Carynthia Kharkongor, T. Chithralekha, Reena Varghese, A SDN Controller with Energy Efficient Routing in the Internet of Things (IoT), Procedia Computer Science, Volume 89, 2016, Pages 218-227.

[13] J. K. Samriya, C. Chakraborty, A. Sharma, M. Kumar and S. K. R, "Adversarial ML-Based Secured Cloud Architecture for Consumer Internet of Things of Smart Healthcare," in IEEE Transactions on Consumer Electronics, vol. 70, no. 1, pp. 2058-2065, Feb. 2024.

[14] D. P. Isravel, S. Silas, J. W. Kathrine, E. B. Rajsingh and J. Andrew, "Multivariate Forecasting of Network Traffic in SDN-Based Ubiquitous Healthcare System," in IEEE Open Journal of the Communications Society, vol. 5, pp. 1537-1550, 2024.

[15] M. Kumhar, J. Bhatia, N. K. Jadav, R. Gupta and S. Tanwar, "AI-based Intelligent SDN Controller to Optimize Onion Routing Framework for IoMT Environment," 2023 IEEE International Conference on Communications Workshops (ICC Workshops), Rome, Italy, 2023, pp. 885-890.

[16] M. Cicioğlu and A. Çalhan, "A Multiprotocol Controller Deployment in SDN-Based IoMT Architecture," in IEEE Internet of Things Journal, vol. 9, no. 21, pp. 20833-20840, 1 Nov.1, 2022.

[17] V. Ravi, T. D. Pham and M. Alazab, "Attention-Based Multidimensional Deep Learning Approach for Cross-Architecture IoMT Malware Detection and Classification in Healthcare Cyber-Physical Systems," in IEEE Transactions on Computational Social Systems, vol. 10, no. 4, pp. 1597-1606, Aug. 2023.

[18] V. Ravi, T. D. Pham and M. Alazab, "Deep Learning-Based Network Intrusion Detection System for Internet of Medical Things," in IEEE Internet of Things Magazine, vol. 6, no. 2, pp. 50-54, June 2023.

[19] A. Ouhab, T. Abreu, H. Slimani and A. Mellouk, "Energy-efficient clustering and routing algorithm for large-scale SDN-based IoT monitoring," ICC 2020 - 2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 2020, pp. 1-6.

[20] Y. Ding, G. Wu, D. Chen, N. Zhang, L. Gong, M. Cao, and Z. Qin, "DeepEDN: A Deep-Learning-Based Image Encryption and Decryption Network for Internet of Medical Things," in IEEE Internet of Things Journal, vol. 8, no. 3, pp. 1504-1518, 1 Feb.1, 2021.

[21] Zabeehullah, N.A. Khan, N.A., J. Iqbal, F.K. Karim, N. Innab, and S.M. Mostafa, "DQQS: Deep Reinforcement Learning based Technique for Enhancing Security and Performance in SDN-IoT Environments," in IEEE Access, vol. 12, pp. 60568-60587, Apr. 2024.

[22] T. P. Lillicrap, J. J. Hunt, A. Pritzel, N. Heess, T. Erez, Y. Tassa, D. Silver, and D. Wierstra, "Continuous control with deep reinforcement learning," arXiv preprint arXiv:1509.02971, 2015, https://doi.org/10.48550/arXiv.1509.02971.

[23] D. Berthelot, T. Schumm, and L. Metz, "Began: Boundary equilibrium generative adversarial networks," arXiv preprint arXiv:1703.10717, 2017, https://doi.org/10.48550/arXiv.1703.10717.

Authorized licensed use limited to: VIT-Amaravathi campus. Downloaded on July 29,2025 at 05:55:58 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.