Blockchain and Reinforcement Neural Network for Trusted Cloud-Enabled IoT Network

Jitendra Kumar Samriya, Surendra Kumar, Mohit Kumar, Minxian Xu, *Member, IEEE*, Huaming Wu, *Senior Member, IEEE*, and Sukhpal Singh Gill

***Abstract*—The rapid integration of Internet of Things (IoT) services and applications across various sectors is primarily driven by their ability to process real-time data and create intelligent environments through artificial intelligence for service consumers. However, the security and privacy of data have emerged as significant threats to consumers within IoT networks. Issues such as node tampering, phishing attacks, malicious code injection, malware threats, and the potential for Denial of Service (DoS) attacks pose serious risks to the safety and confidentiality of information. To solve this problem, we propose an integrated autonomous IoT network within a cloud architecture, employing Blockchain technology to heighten network security. The primary goal of this approach is to establish a Heterogeneous Autonomous Network (HAN), wherein data is processed and transmitted through cloud architecture. This network is integrated with a Reinforced Neural Network (RNN) called ClouD_RNN, specifically designed to classify the data perceived and collected by sensors. Further, the collected data is continuously monitored by an autonomous network and classified for fault detection and malicious activity. In addition, network security is enhanced by the Blockchain Adaptive Windowing Meta Optimization Protocol (BAW_MOP). Extensive experimental results validate that our proposed approach significantly outperforms state-of-the-art approaches in terms of throughput, accuracy, end-to-end delay, data delivery ratio, network security, and energy efficiency.**

***Index Terms*—Internet of Things, reinforcement neural network, heterogeneous autonomous network, cloud computing, control system.**

I. Introduction

IN ADDITION to conventional human-to-human communication scenarios, the advent of mobile communications, particularly 5G and beyond (B5G), will facilitate machine-to-machine communication. This technological progression acts as a pivotal force driving various applications across industries [1], e.g., smart grids, collaborative robots, and cooperative cars for consumers. To adequately serve this diverse range of applications, mobile network operators are obliged to upgrade their network architectures to support a substantial surge in connected devices and an exponential growth in shared data [2]. Thus, networks must accommodate specific use cases with custom architecture to become more agile. The 5G standards development organisations anticipate supporting three key service categories: Massive Machine Type Communication (mMTCs), Enhanced Mobile Broadband (eMBB), and Ultra-Reliability and Low Latency Communication (URLLC) [3]. Traditional system architectures use monolithic systems, which are difficult to maintain and evolution speed. Monolithic systems lack the flexibility to adjust quickly as data demand increases, making them difficult to operate and maintain.

To upgrade a monolith, system administrators must shut down the entire system. Integration regression could cause unexpected delays. Thus, monoliths cannot deliver the agility needed for 5G and B5G, but Software-Defined Networking (SDN) and Network Function Virtualization is useful. (NFV) [4]. However, the cloud is pitching itself as a 5G/B5G enabler and is highly effective for RAN. The cloud delivers virtual but allocated resources using shared capabilities instead of dedicated servers and private computing devices. Cloud resources offer flexibility, faster deployment, updated software, and auto-scalability [5]. The system can handle all service scenarios. It will take years to accomplish this change, so we're introducing automation with AI capabilities into numerous sectors to provide instant value [6]. Machine learning might connect IoT device responses to the physical world. The development of one does not need the development of the other. IoT and Autonomous Computing Systems (ACS) were originally different concepts. For example, smart thermostats operate central heating methods independently based on the presence of consumers as well as their routines.

Manuscript received 23 August 2023; revised 6 November 2023 and 12 December 2023; accepted 25 December 2023. Date of publication 28 December 2023; date of current version 26 April 2024. This work was supported in part by the National Natural Science Foundation of China under Grant 62071327 and Grant 62102408; in part by the Tianjin Science and Technology Planning Project under Grant 22ZYYYJC00020; in part by the Shenzhen Science and Technology Program under Grant RCBS20210609104609044; and in part by the Chinese Academy of Sciences President's International Fellowship Initiative under Grant 2023VTC0006. *(Corresponding author: Huaming Wu.)*

Jitendra Kumar Samriya is with the Department of CSE, Indian Institute of Information Technology Sonepat, Sonepat 131001, India (e-mail: jitu.samriya@gmail.com).

Surendra Kumar is with the Department of Computer Engineering and Applications, GLA University, Mathura 281406, India (e-mail: kumar.surendra1989@gmail.com).

Mohit Kumar is with the Department of IT, Dr. B. R. Ambedkar National Institute of Technology, Jalandhar 144011, India (e-mail: kumarmohit@nitj.ac.in).

Minxian Xu is with the Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences, Shenzhen 518055, China (e-mail: mx.xu@siat.ac.cn).

Huaming Wu is with the Center for Applied Mathematics, Tianjin University, Tianjin 300072, China (e-mail: whming@tju.edu.cn).

Sukhpal Singh Gill is with the School of Electronic Engineering and Computer Science, Queen Mary University of London, E1 4NS London, U.K. (e-mail: s.s.gill@qmul.ac.uk).

Digital Object Identifier 10.1109/TCE.2023.3347690

1558-4127 © 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: TIANJIN UNIVERSITY. Downloaded on April 30,2024 at 08:23:10 UTC from IEEE Xplore. Restrictions apply.

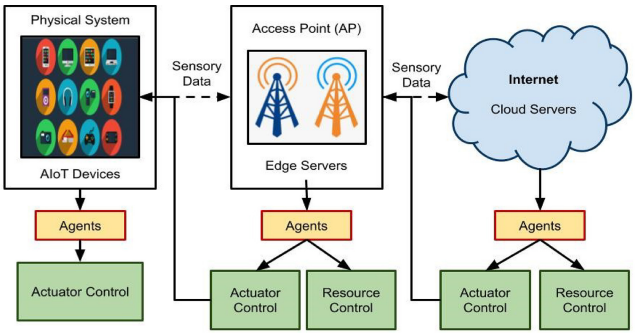

Fig. 1. Autonomous IoT system.

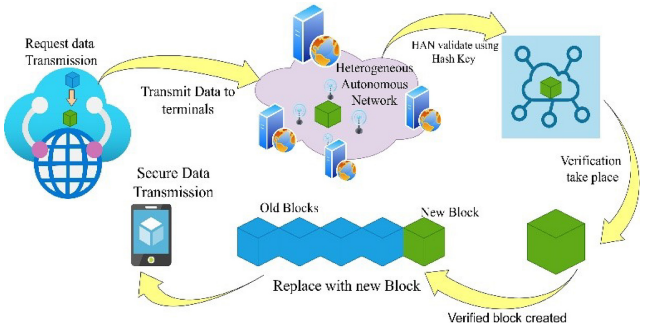

Fig. 2. The integration of blockchain technology with IoT networks.

The integration of 5G and Artificial Intelligence of Things (AIoT) has the potential to usher in a groundbreaking era of connectivity, characterized by their ability to provide ultra-low latency, high data speeds, and extensive device connectivity [7]. This combination, together with the use of Blockchain and Recurrent Neural Networks (RNN), provides a robust ecosystem that improves AIoT application security, scalability, and predictive analytics [8]. Wireless networks connect IoT devices to Access Points (AP), e.g., broadband systems that serve as a gateway to the Internet and host cloud servers [9]. Integrating with the AIoT-5G framework, blockchain allows safe and transparent data sharing between connected devices, reducing security risks and allowing for trustworthy data transactions. RNN, on the other hand, grants devices the ability to record sequential patterns and time-sensitive data, which paves the way for instantaneous judgments and flexible adjustments [10]. Following the acquisition of sensory data that represents a complete or partial condition of the physical method [11]. An AIoT method typically comprises a physical method where AIoT devices with sensors as well as actuators are installed, as depicted in Fig. 1.

A. Motivation and Research Gaps

As demand for IoT services rises, its infrastructure needs a scalable and dependable platform like the cloud to compute and process huge amounts of data. However, IoT networks and cloud-centric computing lack the requirements for services such as latency-aware applications, ubiquitous availability, high bandwidth, and Business Intelligence (BI) [12]. A new approach in IoT applications that enables local and personalised cloud resource management is needed instead of cloud service providers (CSP). Information transactions and data transfers in the IoT network are vulnerable to several attacks, raising security and privacy concerns. The lack of IoT-wireless network trust causes these concerns. Trusted IoT networks that deliver secure and risk-free services are essential.

To resolve the aforementioned issues, a blockchain-based solution is proposed, which involves the implementation of a blockchain-based system, leveraging trustless and immutable public ledgers. A blockchain-based wireless trust avoids wireless attacks and false service record attacks [13]. This technique determines IoT device offloading rates and wireless device processing efficiency, focusing on response time and data integrity. The service record maintained by the serving wireless node broadcasts information about wireless and IoT devices. Utilizing a wireless blockchain, reputations are stored and compensations are allocated accordingly, effectively diminishing the risk posed by selfish node attackers. Blockchain's decentralised ledger eliminates the need for third-party transaction verification. Its integration into the Internet of Things eliminates centralization, improving transparency, autonomy, and safety. Blockchains as universal ledgers enable trust in all intelligent device communications in this design. Nguyen et al. [14] developed a blockchain-based, smart-contract-enabled, cloud-centric architecture for IoT application security. Blockchain technology securely records data in ledgers and stores it in cloud data centres. Automated agreements for cloud data interchange and collaboration support secrecy and integrity, as seen in Fig. 2.

To secure IoT networks, this research shows cloud-based autonomous system integration. Blockchain and Heterogeneous Autonomous Networks (HANs) improve data security and processing efficiency. Use ClouD RNN, a specialised Reinforced Neural Network, to classify sensor data to detect threats. Problems with harmful actions are recognised faster by the autonomous network's continuous monitoring. Cloud networks require scalability and processing complexity, while blockchain's original architecture lacks. Network security and scalability are improved by the Blockchain Adaptive Windowing Meta Optimisation Protocol (BAW MOP). Throughput, precision, and energy efficiency were all optimised in the experimental findings, proving that the suggested method works. Security challenges are addressed include DoS attacks, malware, phishing, code injection, and tampered nodes. These findings offer a comprehensive approach to IoT network safety.

An IoT network control system with a secure data-sharing architecture requires a data owner, blockchain infrastructure, and cloud computing. Managing IoT data and transactions on a permissioned blockchain on top of the cloud-based IoT system allows user access verification and data usage monitoring. Like cloud-based blockchain key management systems, hierarchical access control schemes are being studied. Distributed side blockchains at fog nodes and a cloud-based multi-blockchain would provide efficient network control and flexible storage for scalable cloud IoT networks.

B. Problem Statement

The autonomous IoT network uses blockchain technology to detect faults and malicious activity and improve network

Authorized licensed use limited to: TIANJIN UNIVERSITY. Downloaded on April 30,2024 at 08:23:10 UTC from IEEE Xplore. Restrictions apply.

security to become trusted. The Heterogeneous Autonomous Network (HAN) uses RNN and cloud to categorise fault detection and analyse data. This method works effectively in extensive complex solution domains. Once correctly trained and hyper-tuned, this approach is ideal for high-dimensional data, sparse and delayed rewards, and consumer industrial use cases involving feedback provided after a set sequence of operations. The Blockchain Adaptive Windowing Meta Optimisation Protocol (BAW_MOP) enhances network security.

C. Our Contributions

The main contributions of this paper are four-fold:

- We develop a framework that integrates HAN with the cloud computing paradigm, specifically designed to address IoT use cases. The primary function of this framework is to classify perceived data by using RNN.
- We integrate blockchain technology into underlying networks, as there are implications for fault detection mechanisms and the recognition of malicious activities. This incorporation allows for persistent monitoring to safeguard against potential attacks.
- We propose a novel technique known as the Blockchain Adaptive Windowing Meta Optimization Protocol (BAW_MOP), which can enhance network security.
- We improve Quality of Service (QoS) metrics, including throughput, delay, data delivery ratio, accuracy, network security, and energy efficiency, while considering the number of nodes and the data transmission rate.

The rest of the paper is structured as follows: Section II details the related work, and Section III elaborates on the system model. Section IV presents the enhancement of network security through blockchain-adaptable windowing techniques. Section V demonstrates the performance of the proposed approach. Finally, a conclusion is given in Section VI.

II. Related Work

Babbar et al. [23] conducted a study on 5G network slicing with SDN and NFV, explored the various structures involved in this technology, and also highlighted potential challenges that may arise in the future. Notably, they advocated for the utilization of containerization technologies as a pivotal enabler for the progress of 5G networks. Furthermore, deep learning can improve network quality and consumer experience, while resolving privacy concerns in 5G heterogeneous radio access networks, beyond-RAN networks, and end-to-end network slicing [24]. As a result, Qian et al. [25] proposed a Docker-based microservice-based cloud-native architecture for the prototype. The 5G-EmPOWER platform, which supports complicated policy deployment and management across SDN, was introduced in [26]. They used Long-Term Evolution (LTE) network elements provided by software radio methods to assess the performance of their platform. Gomez et al. [27] described a virtualized 5G structure that supports network slicing as a prototype. Huang et al. [28] looked into the use of an Open-Air Interface (OAI) on top of M-CORD. They also used a monolithic architecture to demonstrate a virtualized 5G RAN and core deployment. Further, the O-RAN Alliance launched an operator-led campaign to open RAN interfaces. MOSAIC-5G [29] was a collection of projects aimed at transforming the RAN as well as the core into an agile service delivery platform that could quickly test new ideas, applications and business demands. Zhang et al. [19] proposed an AI-enabled trusted cloud edge framework, which is designed to enhance the security of computation and transmission due to IoT devices transmitting data to the network edge, which can be a target for various types of modern cyber-attacks.

The convergence of IoT, blockchain, and reinforcement neural networks is transforming industries, offering efficiency, security, and creativity. This paradigm shift accelerates with 5G, which provides high-speed, low-latency connections for IoT devices [30]. High data rates, low latency, and huge device connectivity make 5G crucial for IoT's scalability, latency, and energy efficiency [31]. However, these advances face challenges. Data integrity and security solutions are needed for IoT networks due to security vulnerabilities, data privacy concerns, and trust issues [32]. Blockchain technology provides immutability, transparency, and decentralized consensus for IoT networks. Blockchain topologies designed for IoT applications boost their potential [33]. Integrating these technologies creates new use cases that benefit smart cities, healthcare, and supply chain management [34]. A blockchain, reinforcement neural network, and 5G infrastructure create a future-proof IoT ecosystem. Blockchain protects data integrity, reinforcement learning optimizes resource allocation, and 5G provides fast connectivity [35]. Blockchain's tamper-resistant and auditable ledger supports IoT trust and security. It secures data sharing, manages device identities, and promotes supply chain transparency [36]. This paradigm optimizes IoT resource allocation, energy management, and decision-making through reinforcement learning [37]. Optimizing resource allocation, spectrum sharing, and quality of service management with 5G [38]. However, computational complexity, scalability, interoperability, and regulatory compliance remain. These challenges suggest future studies strengthen this integration and realize its transformational promise [39].

The integration of blockchain, reinforcement neural networks, and 5G for IoT presents challenges such as computational complexity, scalability, interoperability, and energy efficiency. Despite the benefits of blockchain, privacy and security issues still exist. The practical implementation of these systems can be influenced by the need for real-time decision-making, adherence to predefined rules, and constraints related to limited resources. To address these challenges, a Heterogeneous Autonomous Network (HAN) utilizing IoT devices, Deep Neural Networks (DNN), and cloud computing was proposed. A cloud-based Reinforcement Neural Network (ClouD_RNN) is used to classify data from sensor modules, and then another network is used to detect faults and malicious behavior. The use of the cloud for processing and the implementation of the Blockchain-based Adaptive Windowing Meta Optimization Protocol (BAW_MOP) both contribute to a more secure network.

Authorized licensed use limited to: TIANJIN UNIVERSITY. Downloaded on April 30,2024 at 08:23:10 UTC from IEEE Xplore. Restrictions apply.

TABLE I
STATE-OF-ART APPROACHES WITH THEIR CONTRIBUTIONS AND LIMITATIONS

Work	Techniques/Algorithms	Contributions/Advantages	Limitations/Disadvantages
Tsourdinis *et al.* [15]	Deep learning (DL) for UAV	Obstacle detection and collision avoidance	Cloud based DL-UAV framework does not provide a satisfactory solution to IoT applications
Kot *et al.* [16]	Deep Learning for driving control system	Estimate the accuracy and trajectory error	Self-driving autonomous system without IoT technology
Chakraborty *et al.* [17]	ANN for securing integrated cloud fog environment	Detecting abnormal activity, and reducing the possibilities of any vulnerabilities	Theoretically analyze the concept, lack of practical aspects and lack of transparency in the result is an issue.
Wu *et al.* [18]	DL for edge-enabled IoT	Evaluate and analyze the latency, computation and transmission security, overhead	Authors did not discuss the offloading techniques for IoT services and secure the edge-enabled IoT services without blockchain
Zhang *et al.* [19]	Secure framework using federated DL and Blockchain	Improve the accuracy, and loss	Address the IoT data-based privacy and security issues Partially resolve the challenges and need further improvement
Yin *et al.* [20]	LSTM for autonomous vehicles	Identify the intrusions and improve the rate of false alarms, accuracy, recall, precision, etc	The proposed approach is tested for small-scale IoV network, scalability is not guaranteed
Khan *et al.* [21]	Edge computing and stacked LSTM model for IoV	Improve the accuracy, recall and identify the suspicious vehicle behavior	It did not discuss the use of blockchain technology to protect the IoV network in any aspect.
Wazid *et al.* [22]	Blockchain-enabled security framework	Improve better accuracy and F1-score for ransomware attack detection	As new vulnerabilities and attack routes are uncovered, they may require to be regularly updated and revised to allow for consumers.
This Work	Blockchain and RNN for IoT networks	Detect the fault and any malicious behavior, then try to enhance network throughput, accuracy, end-to-end delay, data delivery ratio, and other metrics such as network security	N/A

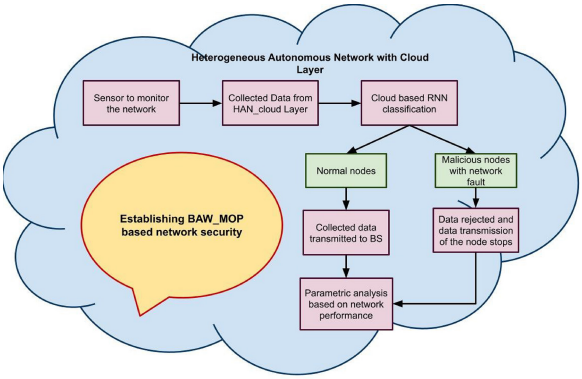

Fig. 3. Proposed architecture of a heterogeneous autonomous network-based control system.

III. SYSTEM MODEL

In this section, the proposed network model for HAN control systems is shown in Fig. 3. The architecture uses network sensor data and cloud-based data classification to detect network failures and malicious nodes. These identified nodes exhibiting malicious activity contribute to the enhancement of network security. The implementation of BAW_MOP along with data optimization further enhances network security.

Initially, all nodes start with the same capabilities, but diverse energy levels emerge post-deployment, and each node is identified by a unique ID. The network nodes can exhibit either homogeneous or heterogeneous characteristics. The nodes lack GPS antennas, and thus are unaware of their location. After deployment, the Sensor Nodes (SNs) operate unattended, preventing any possibility of battery recharging. Within the network, there is a single fixed Base Station (BS) positioned at the center, benefiting from a reliable power source and free from energy, memory, or processing constraints. Utilizing the available received signal intensity, the distance between SNs is computed, thereby establishing symmetrical wireless radio links.

A. Network Model

In an ideal scenario, the number of nodes in a network and their energy levels would be entirely independent. However, in the context of this work, each SN is randomly assigned energy from a specific energy interval, deviating from complete independence between the number of nodes and their energy levels. Even if two SNs initially possess the same amount of energy, it is highly unlikely that they will maintain an identical quantity of energy throughout their operation. The total number of nodes in the network is denoted by N. The secondary parameters in the model are influenced by the value denoted as n. Essentially, the network model should have n secondary parameters to define an n-level heterogeneity. The hierarchy of inequalities is established by the energy levels $E_1 < E_2 < E_3 < \ldots < E_n$. The interconnection among the energy levels of various node types with constant (δ) is described as follows:

$$E_j = E_1(1 + (j-1)\delta), j = 1, 2, 3, \ldots, n \tag{1}$$

where E_1 represents the energy of a type-1 node, and E_j denotes the energy of a j-th node, α is constant calculated by:

$$\begin{aligned} E_{total} = N[&(\alpha-\beta_1)E_1 + (\alpha-\beta_1)(\alpha-\beta_2)E_2 \\ &+ (\alpha-\beta_1)(\alpha-\beta_2)(\alpha-\beta_3)E_3 + \cdots \\ &+ (\alpha-\beta_1)(\alpha-\beta_2)(\alpha-\beta_3)\ldots(\alpha-\beta_n)E_n]. \end{aligned} \tag{2}$$

The fundamental parameter in the model controls the network's heterogeneity level and is related to β_i, $i = 1, 2, \ldots, n$, according to the subsequent formula:

$$\begin{aligned} (\alpha-\beta_1)(1 + (\alpha-\beta_2)(1 + (\alpha-\beta_3)\ldots \\ (1 + (\alpha-\beta_{(n-1)})))) = 1, \end{aligned} \tag{3}$$

where $(\alpha - \beta_i) \leq 1$ and $\beta_i = \beta_{i-1} - 2\Phi$.

For a given level of heterogeneity (Φ), we have

$$\frac{\beta_1}{2(n-1)} > \Phi. \tag{4}$$

Authorized licensed use limited to: TIANJIN UNIVERSITY. Downloaded on April 30,2024 at 08:23:10 UTC from IEEE Xplore. Restrictions apply.

when $\alpha = \beta_2$, the network consists of only one type of node, and the model reflects a 1-level heterogeneity, effectively creating a homogeneous network. The total energy of a 1-level heterogeneous network is defined as follows:

$$E_{1-level} = N(\alpha - \beta_1)E_1. \tag{5}$$

The quantity of type-1 nodes in the network is denoted as $N_1 = N(\alpha - \beta_1)$. When $\alpha = 3$, it models a two-level heterogeneous network whose total energy is calculated by:

$$E_{2-level} = N((\alpha - \beta_1)E_1 + ((\alpha - \beta_1)(\alpha - \beta_2)E_2)). \tag{6}$$

Node type-1 and type-2 in the network are characterized as follows, respectively:

$$N_1 = N(\alpha - \beta_1), \tag{7}$$
$$N_2 = N(\alpha - \beta_1)(\alpha - \beta_2), \tag{8}$$

where $(\alpha - \beta_1) + (\alpha - \beta_1) * (\alpha - \beta_2) = 1$.

When $\alpha = \beta_4$, there exist three non-zero terms, portraying a three-level heterogeneous network, with the total energy determined by:

$$E_{3-level} = N((\alpha - \beta_1)E_1 + (\alpha - \beta_1)(\alpha - \beta_2)E_2 + ((\alpha - \beta_1)(\alpha - \beta_2)(\alpha - \beta_3))E_3). \tag{9}$$

Node type-1, type-2 and type-3 in the network are characterized as follows, respectively:

$$N_1 = N(\alpha - \beta_1), \tag{10}$$
$$N_2 = N(\alpha - \beta_1)(\alpha - \beta_2), \tag{11}$$
$$N_3 = N(\alpha - \beta_1)(\alpha - \beta_2)(\alpha - \beta_3), \tag{12}$$

where $(\alpha - \beta_1)(1 + (\alpha - \beta_2)(1 + (\alpha - \beta_3))) = 1$ and the associated condition is given by:

$$E_{i-level} = N(\alpha - \beta_1)E_1 + (\alpha - \beta_1)(\alpha - \beta_2)E_2 + \ldots + (\alpha - \beta_1)(\alpha - \beta_2)(\alpha - \beta_3)\ldots(\alpha - \beta_i)E_j), \tag{13}$$
$$N_1 = N(\alpha - \beta_1), \tag{14}$$
$$N_2 = N(\alpha - \beta_1)(\alpha - \beta_2), \tag{15}$$
$$N_3 = N(\alpha - \beta_1)(\alpha - \beta_2)(\alpha - \beta_3)((\alpha - \beta_1)(1 + (\alpha - \beta_2)(1 + (\alpha - \beta_3)\ldots + (1 + (\alpha - \beta_i - 1))))) = 1. \tag{16}$$

B. Cloud Architecture-Based Data Classification Using Reinforcement Neural Network (ClouD_RNN)

The Neural Network (NN) model is utilized to find patterns in data streams. The result of the current state is anticipated based on the output of previous states, although the feed-forward NN computes in a single direction from input to output. RNN models are more feasible for real-time implementation due to their significantly reduced execution time, even though their performance is more effective than other models in terms of throughput, authentic consumers, and fairness metrics. In the network architecture depicted in Fig. 4, the layers include the input layer, followed by the RNN layer, Mapping layer, Background layer, De-mapping layer, and finally the output layer. The RNN layer uses the Sigmoid activation function to produce output values,

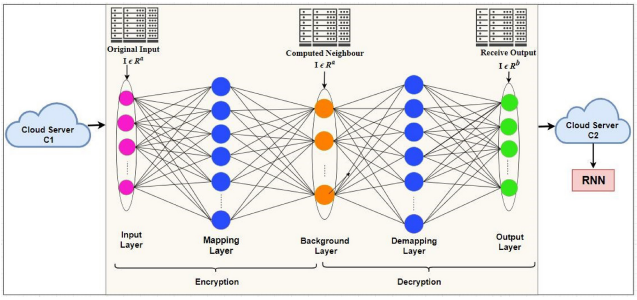

Fig. 4. The system architecture with the RNN model.

which are processed to derive anticipated values. Binary cross-entropy loss is computed to evaluate the loss in predictions, ultimately providing the final results in the output layer.

Interactions with the IoT environment occur in discrete time steps, whereas learning in NN happens in real time. In a conventional Reinforcement Learning (RL) cycle, the agent engages by receiving environment states and choosing actions (a_t). Then, in response to the activity carried out by the IoT environment state, a new state $(s_t + 1)$ is created. The agent may or may not receive the reward $(r_t + 1)$ for the selected action, and the agent may additionally identify the transition $(a_t, s_t + 1)$. After each cycle, the agent updates the action value function (s, a) or value function $V(s)$ according to a policy. By presenting the policy, reward function, state value function pairs, and policy, the most probable solution to the RL problem is presented. The value functions are classified as either action-value functions (Q) or state-value functions (V). Predictions for expected outcomes are conducted within the state-value function, using the policy π and state s. The incentives are applied at subsequent time steps to identify the policy using the given discount factor $(\gamma \in [0, 1])$, which is defined as:

$$V^{\pi}(s) = E_{\pi}\Big(\sum_{k=0}^{n} \gamma^k r_{t+k+1} | \; s_t = s\Big). \tag{17}$$

The prediction of expected outcomes is conducted by the action-value function, where the policy π is computed by summing rewards for each state-action pair s, as shown below:

$$Q^{\pi}(s, a) = E_{\pi}\left(\sum_{k=0}^{n} \gamma^k r_{t+k+1} | \; s_t = s, a_t = a\right). \tag{18}$$

The ideal policy has been achieved, and the Markov Decision Processes (MDP) have been solved using the dynamic state-value function. In some simple instances, the Bellman expectation equation is used to estimate the state-value function for a given policy, as shown below:

$$V^{\pi}(s) = E_m\big(r_{t+1} + \gamma V^{\pi}(s_{t+1}) | \; s_t = s\big). \tag{19}$$

The goal of the policy evaluation process is to maximize state-action values to derive the most effective policy π. However, when the environment is unknown, model-free methods are utilized instead of relying on MDP. In some circumstances, the action value is maximized rather than the state value, as shown below:

$$Q^{\pi}(s, a) = E_n\big(r_{t+1} + \gamma Q^{\pi}(s_{t+1}, a_{t+1}) | \; s_t = s, a_t = a\big). \tag{20}$$

Authorized licensed use limited to: TIANJIN UNIVERSITY. Downloaded on April 30,2024 at 08:23:10 UTC from IEEE Xplore. Restrictions apply.

C. Cloud Architecture

The cloud architecture comprises several components, including cloud servers and (many) customers. Authenticated customers encrypt trained images and non-readable image data, sending these to the cloud servers. Subsequently, the server receives a content-based query image from the consumers. The encrypted data is stored on cloud servers, which perform content-based image retrieval using a large cloud database requiring less computational power.

As depicted in Fig. 4, two cloud servers C1 and C2, are configured to identify the optimal policy and its value in the following manner. Initially, they either iteratively enhance the initial policy as a policy iteration or recursively refine the arbitrary value function to compute the better action value, utilizing it to store the encrypted sub-pictures. In general, the linear layers of the pre-trained RNN model output images undergo several heterogeneous processes. C1 keeps its private keys k, and its operations are performed in C2 to execute computations involving high security on the non-linear layers. The interaction involves the exchange of the model's features between the C1 and C2 cloud servers, followed by the encryption of photos, respectively. consumers intact the similar Nearest Neighbour (SNN) query on the unintelligible images together. The trained model transforms into an encrypted data format by the consumers and detects a test image by encrypting the photographs provided by the consumers. However, the trained image I consumer obtains the encrypted image I_a by summing a stochastic matrix I_b along with it. However, I_a is transferred to the cloud server C1, and I_b is transmitted to C2. A client makes over the test image trapdoor in the same way as the exploratory SNN images. C1 then uses BAW_MOP with C2 to transform the unintelligible image I_b to the primary image with key s_k, which is then accepted I_a.

The architecture of the Q network is defined by the complexity and the size of the training dataset. The Q network's input aligns with the structure of the training sample, and the number of outputs corresponds to the number of sample classes. Essentially, the Q network, in its form without the last softmax layer, functions as an NN classifier. The training process of the Q network is described in Algorithm 1. The deep Q-learning algorithm completes approximately 120,000 iterations. The parameters of the converged Q network are saved, and when combined with a softmax layer, it is considered an NN classifier trained on skewed data.

IV. Network Security With Data Optimization Using BAW_MOP

The key privacy aims of BAW_MOP are: i) Keeping local data points within devices to prevent them from being exposed to external entities, ii) Safeguarding local data from the server by not divulging individual local method updates to it, and iii) Ensuring that irrelevant internal and external entities are excluded from local and global model modifications. Under the security goals, the aims are to ensure the security and integrity of committed clients' local method updates and to verify the provenance of model updates.

Algorithm 1 ClouD_RNN

Input: Training data $D{=}(x_1, l_1), (x_2, l_2), \ldots, (x_T, l_T)$
Output: Trained parameters θ of the ClouD_RNN model; Start experience replay memory M; Start simulation environments ϵ
Randomly initialize parameters θ
for episode $k = 1$ to K **do** Rearrange training data D
  for $t = 1$ to T **do** Start state $s_1 = x_1$
    Select an action based ϵ-greedy policy: $a_t = \pi_\theta(s_t)$ $r_t, terminal_t = STEP(a_t, l_t)$
    Set $s_{t+1} = x_{t+1}$
    Store $(s_t, a_t, r_t, st + 1, terminal_t)$ to M
    Randomly sample $(s_j, a_j, r_j, s_{j+1}, terminal_j)$
    Perform a gradient descent step on $L(\theta)$ w.r.t. θ: $L(\theta) = \big(y_j - Q(s_j, a_j; \theta)\big)^2$
    if $terminal_t = True$ **then** L break
    end if
    Function STEP($a_t \in A, l_t \in L$)
    Initialize $terminal_t = False$
    if $s_t \in D_p$ **then** ▷ D_p represents the minority class sample set
      if $a_t = l_t$ **then** Set $r_t = 1$
      else
        Set $r_t = -1$
        if $a_t = l_t$ **then** Set $r_t = \lambda$
        else if $LSetr_t = -\lambda$ **then** return r_t and $terminal_t$
        end if
      end if
    end if
  end for
end for

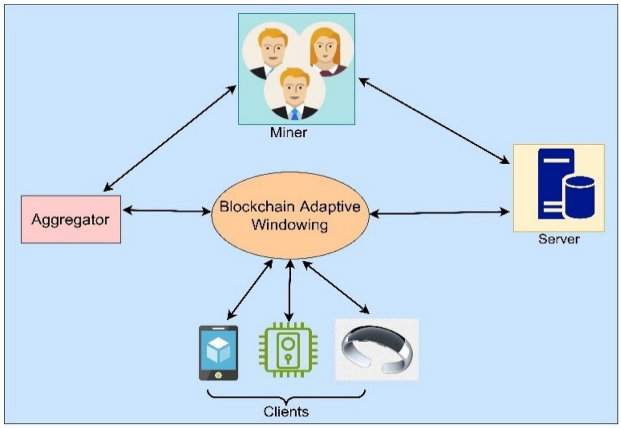

Fig. 5. Architecture of BAW_MOP.

We propose a BAW_MOP architecture, as illustrated in Fig. 5, which incorporates five components focused on ensuring both security and privacy protection. One of its aspects involves a technique for training a privacy-preserving LR method using vertical adaptive windowing. This approach is particularly beneficial when two datasets share the same sample ID space but have varying feature spaces. This scenario is defined as:

$$X_i \neq X_j, Y_i \neq Y_j, I_i \neq I_j, \forall D_i, D_j, i \neq j, \tag{21}$$

$$X_i \neq X_j, Y_i \neq Y_j, I_i \neq I_j, \forall D_i, D_j, i \neq j. \tag{22}$$

The adaptable windowing technique implemented across three blockchains offers flexibility, allowing its application in diverse IoT scenarios based on specific requirements. In the

Authorized licensed use limited to: TIANJIN UNIVERSITY. Downloaded on April 30,2024 at 08:23:10 UTC from IEEE Xplore. Restrictions apply.

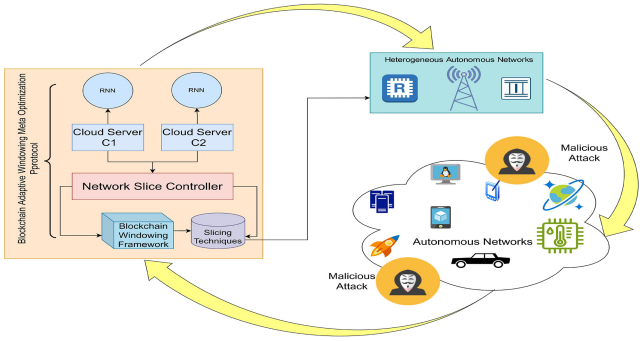

Fig. 6. Proposed HAN-based cloud architecture integrated with ClouD_RNN.

context of various industrial situations, data is channeled into a local model. The local model is then updated by uploading its outcomes to the global aggregation process, depicted in Fig. 6. The federation model takes the global outcomes as its input. To standardize the data object within the dataset, a 0-1 standardization process is employed, transforming data from various dimensions into the [0, 1] dimension with $\bar{x}$ state. This conversion is achieved through the following mapping function:

$$\bar{x} = \frac{x - min_i}{max_i - min_i}, i = 1, 2, \ldots, k. \tag{23}$$

For an arbitrary dimensionality in a data object, the maximum is "1" and the minimum is "0" in the dataset after normalization. Before running the clustering method, data normalization is used to improve convergence speed and accuracy. As a result, the server can't retrieve individual local changes from the ledger; instead, it can only recover aggregated values once the aggregator collects updates and re-encrypts them with the transformation key. Despite the lower influence on classification accuracy, the goal here is to protect sensitive private data when large datasets are classified. To begin, the specified privacy budget is divided evenly across all trees in the forest and it is given as:

$$\epsilon' = \frac{\epsilon'}{n_{trees}}. \tag{24}$$

Given that the samples were randomly selected, there may be some overlap. Additionally, the privacy budget ϵ for each tree is uniformly distributed across each tier using Eq. (25).

$$\epsilon'' = \frac{\epsilon}{max\_depth + 1}. \tag{25}$$

The blockchain keeps track of encrypted model revisions, allowing clients' contributions to the globally optimized model to be tracked and verified. The verifier, in particular, can retrieve all of a client's updates in a batch and produce an aggregate without the suspect client's input. The established fundamental verification function in the preliminary experiment, in which the server acts as a verifier, evaluates gradients after recovering aggregate in each round.

In this technique, a less cost-based spanning tree is built between CHs and sinks.

a) Initiate CH_s as the starting point for virtual ants, with the sink as the designated endpoint.

Algorithm 2 For BAW_MOP

Input: encrypted dataset $D' = x^{(i)} | 0 \le i \le n$ (privacy budget is $\frac{\epsilon}{2n}$; positive integer $g = n + 1$), clustering number k.
Output: center, $c | x^{(i)} \in D', i = 0, \ldots, n; 0 \le c \le k$.
Get_centroids $\mu_j, 0 \le j \le k$
while $J(c, \mu) \ne \sum_{i=1}^{m} ||x^{(i)} - \mu_c i)||^2$ **do**
  for $c = 1$ to k **do**
    $c^{(i)} = \arg\min_j \left\| x^{(i)} - \mu_j \right\|^2$
    for $j = 0$ to k **do**
      $\mu_j = \frac{\sum_{i=1}^{n} x^{(i)} | c_i = j}{\sum_{i=1}^{n} 1_\epsilon (i - j)}$
    end for
  end for
end while
return center

b) The quantity of pheromones on the paths between CH_s distances determines the range that virtual ants can travel.

c) The initial step in the Minimum Cost Optimization Problem (MOP) might involve trail collection between adjacent clusters, accomplished by simulating synthetic nodes from CH_s towards the sink.

d) The subsequent group of nodes can analyze the pheromone deposits left by previously successful node routes and navigate to take the most efficient path.

e) When the node moves from CH_i to CH_j, the selection principle for a regular node is determined as:

$$P_{ij} = \frac{(\tau_{ij})^x + (\eta_{iu})^l}{\sum (\tau_{ij})^x (\eta_{ij})^l}. \tag{26}$$

where τ_{ij} is used to update the quantity of pheromone from transmission state i to j, $x \ge 0$ controls heuristic visibility function τ_{ij} and $l \ge 1$ controls the transmission state η_{iu} and can be adjusted.

f) If a link exists between two CH_s, then P_{ij} will be updated; otherwise, P_{ij} will be set to 0. Calculate the Euclidean Distance between CH_i and CH_j using the following formula:

$$D_{ij} = \sqrt{\left[CH_i - CH_j) \cdot xq\right]^2 + \left[(CH_i - CH_j) \cdot yq\right]^2}. \tag{27}$$

g) All nodes that have successfully reached the Base Station (BS) will update their D_{ij} values. The pheromone evaporation (q) on the boundary between CH_i and CH_j is $\tau_{ij} - (1 - \rho)\tau_{ij}$. The evaporation process is a prerequisite before adding P. This step supports the identification of the shortest path and guarantees that no other path is regarded as the shortest. The degree of pheromone evaporation is determined by the value of q.

h) MOP does not select CHs, causing a rapid decrease in the quantity of P.

i) When all nodes reach the sink during each iteration, the value of τ_{ij} is calculated as:

$$\tau_{ij}(t + n) = \rho\tau_i(t) + \Delta t_{ij}, \forall t = 1, 2, \ldots, n, \tag{28}$$

Authorized licensed use limited to: TIANJIN UNIVERSITY. Downloaded on April 30,2024 at 08:23:10 UTC from IEEE Xplore. Restrictions apply.

TABLE II
SIMULATION SETUP

Description	Symbol	Value
BS position	S_p	(50, 50)
No of sensors	N	100
Threshold distance	d_0	70 m
Energy consumed by the amplifier to transmit messages (long distance)	ϵ_{mp}	0.0013 nJ/bit/m^4
Initial energy	E_1	0.2 J
Cluster radius	C_r	25 m
Energy consumed by electronics circuit	E_{elec}	50 nJ/bit
Constants	$\alpha\, and\, \phi$	0.5 and 0.025
Energy consumed by the amplifier to transmit message at a shorter distance	q_{Es}	10 nJ/bit/m^2
Simulation time	S_t	900 s
Secondary model parameter value	β_1	0.4
Bandwidth	B_w	1 Mbps
Data packet size	D_{ps}	512 bits
Message size	L	4000 bits

where ρ is the pheromone evaporation distance and Δt_{ij} denotes the quantity of deposited pheromone. τ_{ij} can be calculated as:

$$\tau_{ij} \leftarrow (1-\rho)\tau_{ij} + \sum_{k=1}^{m} \Delta\tau_i^{\bar{x}}, \tag{29}$$

where m is an optimal path and $\tau_i^{\bar{x}}$ represents the visited edges.

j) Finally, we obtain the quantity of visited edges as follows:

$$\Delta\tau_{ij}^{x} = \begin{cases} 1/C^x \\ 0 \end{cases} \tag{30}$$

where the path with the lowest C^x value is chosen as the initial solution and x uses the path $i \rightarrow j$ for the optimal distance.

V. PERFORMANCE EVALUATION

To evaluate the performance of the proposed approach, we employed an Intel Xeon system with the Processor E5-2640 (2.50 GHz) and 16 GB of primary memory for the experimental simulation. Our simulations, performed using MATLAB, involved deploying 100 Sensor Nodes (SNs) randomly within a square area measuring $100 \times 100m^2$ with dataset.[1] In this scenario, the concept of a distributed blockchain network consisting of 100 nodes, where the starting trust value for each node is 1. For every block time, we've fixed the BS position at 50. After the first ten nodes with the same trust value are found, choose the nodes with the most feedback for inclusion. To commit violations like broadcasting transactions involving lacking service and disclosing fault scores, a subset of nodes N must be malicious. Table II summarizes the input parameters used in our simulations for configuring the model. Our dataset comprises metrics obtained from connected devices like smartphones and IoT technology, among other network and device attributes. Common metrics for consumer QoS, such as data transfer speed, power consumption, and network safety, are derived from the control packets that carry consumer data within the network. These metrics are conveniently accessible as our model operates locally within the network.

[1]https://github.com/adtmv7/DeepSlice

TABLE III
NETWORK-BASED CONTROL SYSTEM OF THROUGHPUT

No. of Nodes	OAI	M-CORD	ClouD_RNN-BAW_MOP
0	61.14 ± 2.3	68.25 ± 2.3	**81.45 ± 3.8**
25	64.27 ± 2.9	72.62 ± 3.0	**85.59 ± 2.6**
50	66.91 ± 3.11	74.75 ± 2.8	**86.98 ± 2.9**
75	67.34 ± 3.8	76.24 ± 2.9	**89.14 ± 2.3**
100	69.57 ± 2.9	81.60 ± 3.2	**94.70 ± 2.7**

TABLE IV
NETWORK-BASED CONTROL SYSTEM OF ACCURACY

No. of Nodes	OAI	M-CORD	ClouD_RNN-BAW_MOP
0	65.04 ± 2.61	71.95 ± 2.21	**75.05 ± 3.47**
25	69.11 ± 2.18	75.78 ± 3.30	**79.56 ± 2.5**
50	70.91 ± 3.18	78.65 ± 2.8	**85.88 ± 2.6**
75	72.43 ± 3.08	85.47 ± 2.11	**88.19 ± 2.02**
100	79.87 ± 2.9	89.96 ± 3.1	**95.67 ± 2.4**

TABLE V
COMPARISON OF NETWORK PACKET END-TO-END DELAY

Data Transmission Rate	OAI	M-CORD	ClouD_RNN-BAW_MOP
0	81.28 ± 2.8	75.62 ± 3.0	**69.29 ± 2.6**
25	74.42 ± 3.1	73.75 ± 2.8	**67.77 ± 2.9**
50	68.89 ± 3.4	67.53 ± 3.5	**59.60 ± 3.4**
75	67.34 ± 3.8	62.24 ± 2.9	**57.14 ± 2.3**
100	53.57 ± 2.9	50.60 ± 3.2	**38.70 ± 2.7**

TABLE VI
COMPARISON OF NETWORK SECURITY ANALYSIS

Number of Nodes	OAI	M-CORD	ClouD_RNN-BAW_MOP
0	70.04 ± 2.8	78.9 ± 2.7	**81.96 ± 3.3**
25	75.17 ± 2.7	82.32 ± 2.9	**85.88 ± 2.4**
50	82.41 ± 3.8	84.95 ± 2.02	**87.98 ± 2.5**
75	85.04 ± 2.97	88.43 ± 2.71	**88.53 ± 2.2**
100	88.89 ± 2.27	91.60 ± 2.08	**98.93 ± 2.06**

We used a dataset that is trained by the Cloud-RNN model to simulate the performance of HAN and BAW MOP techniques. Once trained and optimized, this method excels at handling high-dimensional input, learning with sparse and delayed rewards, and receiving feedback after a predetermined series of operations, all of which are common in consumer industrial enterprises. To integrate the data into our model, we sequenced the consumers in each run and trained the two RNN models using the allocation results from BAW-MOP as labels. Training uses 67% of the set, while testing uses 33%. Using both deep learning-trained images and stock images, information is encrypted before being sent to cloud services by authorized clients. Thereafter, the server gets a content-based query picture from the clients. The encrypted data is kept on cloud servers so that content-based picture recovery can be done using very large cloud datasets that use slightly less energy.

The comparative analysis of suggested and existing methods of control systems for autonomous networked systems is shown in Tables III, IV, V and VI. In the wireless

Authorized licensed use limited to: TIANJIN UNIVERSITY. Downloaded on April 30,2024 at 08:23:10 UTC from IEEE Xplore. Restrictions apply.

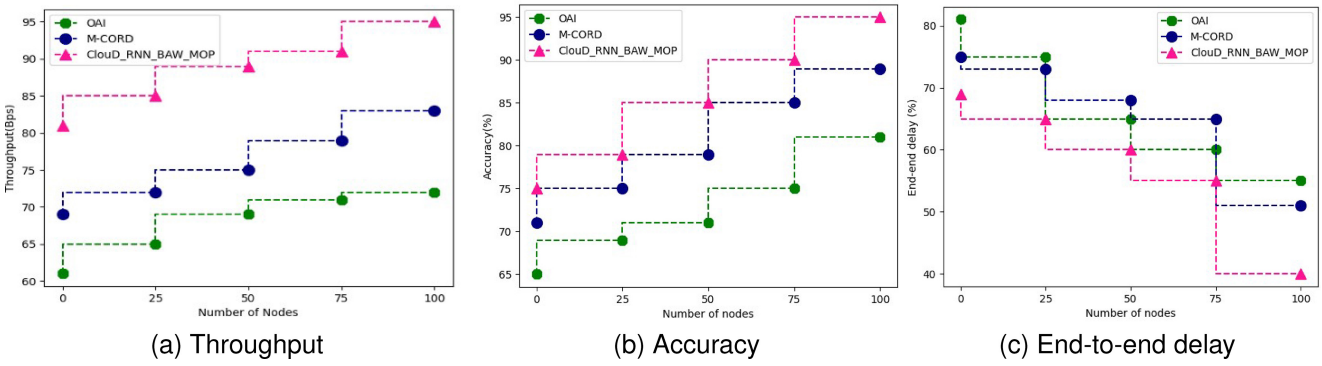

Fig. 7. A comparative analysis of autonomous network-based control system based on no. of nodes in terms of (a) throughput, (b) accuracy, (c) end-to-end delay.

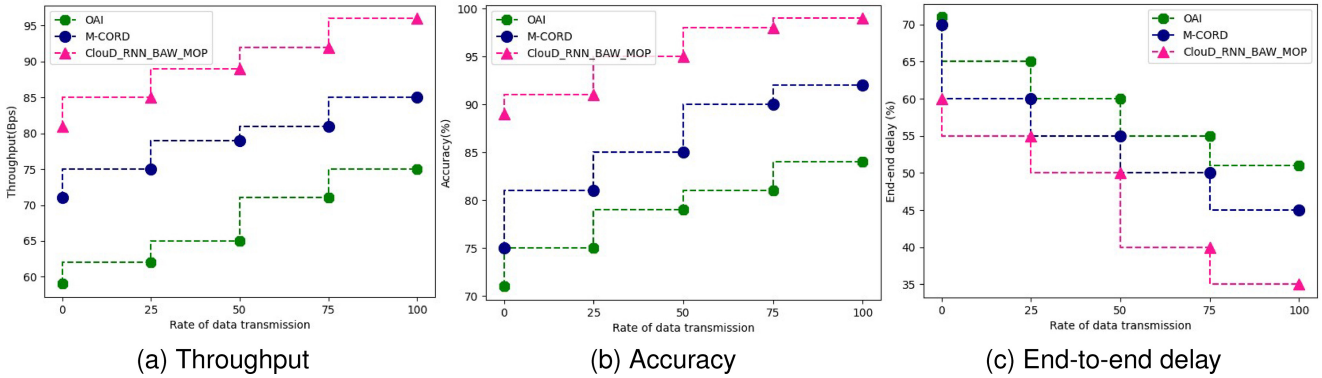

Fig. 8. A comparative analysis of autonomous network-based control system based on rate of data transmission in terms of (a) throughput, (b) accuracy, (c) end-to-end delay.

network, throughput is represented as the number of packets that are successfully transmitted. If we assume that "rate" denotes throughput, then "inventory" equals "rate" multiplied by "time", which is the most basic formula for determining throughput efficiency. The throughput of the wireless network improves the data transmission rate. Increases in the throughput of wireless networks indicate that more data may be successfully transmitted in the same amount of time. The physical layer parameters of the network can be optimized, better modulation techniques used, the signal-to-noise ratio increased, interference decreased, and more efficient data transmission protocols implemented. The comparative analysis clearly shows that the ClouD_RNN with BAW_MOP is the most significant approach from both the OpenAirInterface (OAI) and Mobile Central Office Re-architected as a Datacenter (M-CORD) respectively and also a well-known energy efficient protocol as well. Both OAI and M-CORD are essential initiatives in the telecoms sector, contributing to the development of mobile communication technologies as well as the progression of network topologies towards solutions that are more flexible and software-driven. Network working environments depend on when the initial and last nodes in the network are exhausted. The designed techniques have significant improvements in energy consumption to other compared techniques. Since wireless networks are deployed randomly, the results have some fluctuations and variations, which are denoted with the help of ±. Here, the monitoring of the control system and malicious fault detection have been analyzed in terms of throughput, accuracy, end-to-end delay, data delivery ratio, network security and energy efficiency for the number of nodes and data transmission rate. The period that is needed for a data packet to be transmitted from its point of origin to its endpoint is known as its end-to-end delay. In contrast to Round-trip time (RTT), such a term used in IP network analysis only counts the time it takes for data to travel in only one path, from base to endpoint. Network efficiency refers to the greatest quantity of data that can be sent via an autonomous network to a specific set of consumers per second and still maintaining a satisfactory level of operation. Accuracy measures how well our method did in making predictions. The percentage of network packets that were successfully delivered after being sent is known as the data delivery ratio.

Figs. 7-10 illustrate a comparative analysis of an autonomous network-based control system for monitoring and detecting malicious faults. This analysis evaluates various parameters, including throughput, accuracy, end-to-end delay, data delivery ratio, network security, and energy efficiency. The comparison is based on variations in the number of nodes within the network and the data transmission rate. The proposed technique obtained throughput up to 95%, accuracy up to 95%, end-to-end delay up to 40%, data transmission rate up to 69%, network security up to 95% and energy efficiency up to 95% as the number of nodes increased up to 100. The proposed approach optimized the throughput up to 35.71%, accuracy up to 18.75%, end-to-end delay up to 27.27%, data transmission rate up to 38%, network security up to 13.04% and energy efficiency up to 13.04% compared

Authorized licensed use limited to: TIANJIN UNIVERSITY. Downloaded on April 30,2024 at 08:23:10 UTC from IEEE Xplore. Restrictions apply.

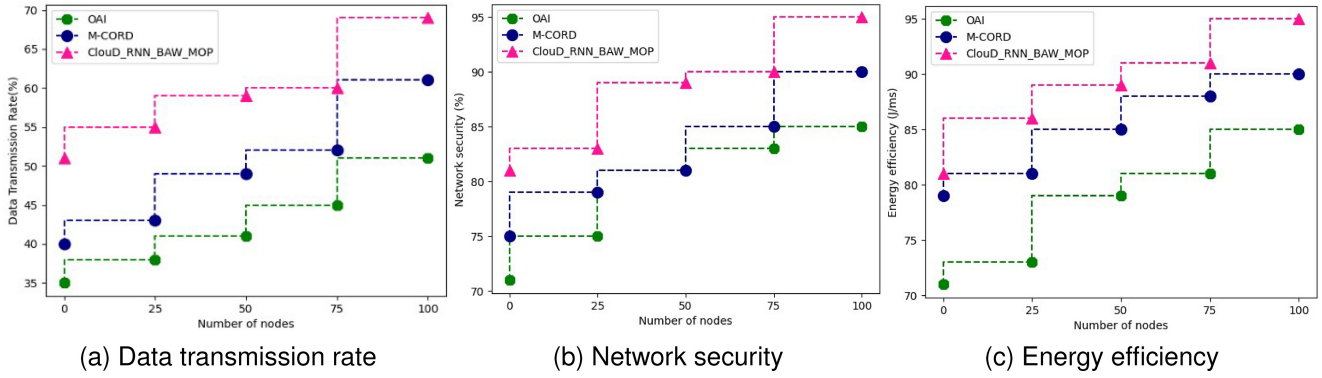

Fig. 9. A comparative analysis of autonomous network-based control system based on no. of nodes in terms of (a) data transmission rate, (b) network security, (c) energy efficiency.

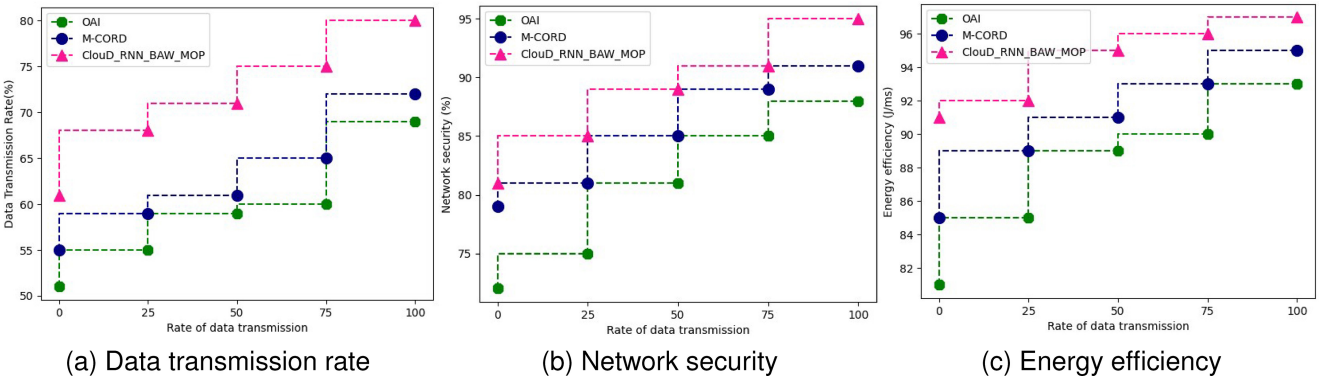

Fig. 10. A comparative analysis of autonomous network-based control system based on rate of data transmission in terms of (a) data transmission rate, (b) network security, (c) energy efficiency.

TABLE VII
RESULTS IMPROVED BY PROPOSED APPROACH COMPARED WITH BASELINE APPROACHES

Based on No. of nodes		Based on data transmission rate	
Parameters	Percentage Improvement	Parameters	Percentage Improvement
Throughput	**35.71%**	Throughput	**29.72%**
Accuracy	**18.75%**	Accuracy	**17.85%**
End to end delay	**27.27%**	End to end delay	**22.22%**
Data Transmission Rate	**38%**	Data Transmission Rate	**17.64%**
Network Security	**13.04%**	Network Security	**9.19%**
Energy Efficiency	**13.04%**	Energy Efficiency	**9.87%**

with baseline algorithms. The proposed technique obtained throughput up to 96%, accuracy of 99%, end-to-end delay of 35%, data transmission rate of 80%, network security of 95%, and energy efficiency of 97% based on the data transmission rate. The QoS parameters have been improved by the proposed approach throughput up to 29.72%, accuracy up to 17.85%, end-to-end delay up to 22.22%, data transmission ratio up to 17.64%, network security up to 9.19% and energy efficiency up to 9.87% as compared with baseline approaches. Table VII depicts the improvement of results in percentage form. The proposed technique obtained optimal results under varying numbers of nodes and data transmission rates.

This study develops and secures conventional approaches for wireless communications operations. if 5G networks use IoT HAN and deep learning with cloud architecture. Security is essential in 5G networks. To address this, we proposed HAN and BAW_MOP techniques. These methods not only demonstrate efficiencies in resource utilization, such as data storage and network bandwidth speed, but also provide robust and optimal security assurances for the network. Information collected from IoT sensors within wireless networks, alongside the cloud-designed information framework, is utilized for identifying network faults and potential malicious points. Following the characterization process, nodes displaying malicious behavior are identified. Subsequently, network security is improved by using the blockchain adaptive windowing meta-optimization protocol (BAW_MOP) alongside the data optimization. BAW_MOP algorithm ensures against different kinds of safety parameters, including those of (a) privacy protection of the information within the sight of attackers who might have the option to read the information with addressed energy levels $E_1 < E_2 < \ldots < E_n$, (b) getting the information from malicious defilement when an attacker can manipulate the information, (c) safely sending information across a wireless network, and (d) safeguarding the security of any demand made to a dataset by the client. Our BAW_MOP approach is functional from a computational complexity and execution point of view, and is likewise demonstrated to be hypothetically ideal regarding the different resources within reach.

To check the node tempering, if the length of the compromised light node is larger than the average length of the mining nodes, then the Power of work (PoW)

Authorized licensed use limited to: TIANJIN UNIVERSITY. Downloaded on April 30,2024 at 08:23:10 UTC from IEEE Xplore. Restrictions apply.

verification has succeeded and required high. Both PoW and Proof-of-Stake (PoS) rely on computational power to resolve issues. Because of this, permissionless blockchain consensus methods are computationally and time-intensively expensive to defend against attacks. Proof-of-Device (PoD) is an identity-based consensus mechanism that enables devices to use their distinct identifiers to choose newly created blocks. Since miners in PoD only have to check a hash function that once for each timestamp, the computational difficulty is lower compared to PoW. Even if a single consumer or group were to own a majority of a network's devices, they would still be unable to exert complete control over the blockchain. This light node will have no eligible peers and communicate its immediate transactions to none until the conventional chain is extended. Single login credentials can authenticate and grant access permissions to all IoT-based services and applications in a cloud platform, preventing consumers from being contacted again. However, CSP requires Multi-Factor Authentication, requiring consumers to use various forms of identification and access control. BAW_MOP is a blockchain-based signature-based detection mechanism for 5G HAN threats. Known Web-based attack types like Structured Query Language (SQL) Injection, Cross-Site Scripting (XSS), and Command Injection can be spotted with the help of BAW_MOP's detection using signatures. Each ClouD_RNN server has the Multi Chain tool applied to contain a blockchain node. To detect attacks against 5G HAN online apps, both the signature list stored in the Web application and the signature list stored on the blockchain are used. Protecting against DoS attacks can be achieved by BAW_MOP's based mitigation strategies including traffic classification, load balancing, and rate limiting. Distributing traffic and mitigating the impact of an attack can be achieved through content delivery networks by using blockchain-based adaptive windowing meta-optimization protocol. Autonomous network-based control system in monitoring and malicious fault detection based on the number of nodes in the network and the data transmission rate.

Using Cloud-RNN we tested scalability, and optimal network performance, a customer using the update feature will see their evaluated transmission added to the log in a few blocks. When this is used in the real-life environment [40], connection delays between consumers and slot heads of state could cause a transmission to be left out of the phase. To fix this problem, we can raise the number of slots and connections to peers for the consumer Integrity node at the accumulation stage. To fix the revelation problem, we can raise the number of slots and connections to peers for the consumer Integrity node at this time. Consider implementing a threshold encryption method to enhance efficiency and mitigate against decryption failure caused by stakeholders who fail to update their decryption keys.

The system consists of diverse components, encompassing cloud servers (C1 and C2) and multiple client entities. Using deep learning-trained images along with stock images, information undergoes encryption and is subsequently transmitted to the cloud servers by authorized clients. Following this, the server retrieves a content-based query image from the clients. The encrypted information is stored on cloud servers to execute content-based image recovery by utilizing huge cloud datasets with less energy consumption. In particular, the linear layers of the pre-trained RNN model result images are imposed on various heterogeneous processes. C1 keeps its private keys k and the IIES operation is applied in C2 to decide the computations with high security on the non-linear layers. Where the cloud servers C1 and C2 transfer the model's elements and encrypt the images, individually. Clients unblemished the Similar Nearest Neighbor (SNN) query based on the illegible images together. The trained deep learning model is changed to encrypt information designed by clients and distinguishes a test image by encrypting images given by clients. However, with the trained images, I client gets the encrypted image I_a by computing a stochastic matrix I_b alongside it. So, I_a is moved to the cloud server C1, and I_b is passed on to C2. A client makes over the test image a secret entrance similar to the exploratory SNN images. C1 then, at that point, utilizes BAW_MOP with C2 to change the illegible image I_b to the essential image with a key s_k, which is then acknowledged I_a.

VI. Conclusion and Future Work

IoT has become a prominent technology in the last decades to offer services and create smart environments like smart homes, cities, transportation, autonomous vehicles, healthcare, etc for consumers. Security and privacy along with energy consumption and latency are major challenges with IoT devices due to resource constraint nature. Cutting-edge technologies exist to address these issues and offer better services. The proposed approach used cloud computing, blockchain technology and deep learning to overcome the modern attacks in IoT networks and optimize QoS parameters. We have designed and developed a heterogeneous autonomous network (HAN) that collects data from the sensor modules, classified using a cloud-based reinforcement neural network (ClouD_RNN). The IoT network is monitored continuously to detect abnormal or malicious activity by the control system. The blockchain-based adaptive windowing meta-optimization protocol (BAW_MOP) is used in heterogeneous IoT networks, where data is processed via the cloud paradigm, to increase network security. The data transmission rate and number of nodes were used to analyze the experimental results. The proposed technique performs outstanding compared with other approaches and improved the given QoS parameters like throughput up to 35.71%, accuracy up to 18.75%, network security up to 13.04% and energy efficiency up to 13.04%, etc. for the number of nodes. For the data transmission rate, throughput up to 29.72%, accuracy up to 17.85%, end-to-end delay up to 22.22%, etc, as compared with baseline approaches. The proposed work used a deep learning-based model that lacks transparency and trustworthiness in the results, we can improve it using explainable AI in the future. In the future, we will reduce the complexity and focus on lightweight encryptions as well as hashing schemes with modified blockchain. Furthermore, deep learning algorithms are used to accurately collect data from Industry 5.0 environments.

Authorized licensed use limited to: TIANJIN UNIVERSITY. Downloaded on April 30,2024 at 08:23:10 UTC from IEEE Xplore. Restrictions apply.

REFERENCES

[1] S. Singh, C. R. Babu, K. Ramana, I.-H. Ra, and B. Yoon, "BENS-b5G: Blockchain-enabled network slicing in 5G and beyond-5G (b5G) networks," *Sensors*, vol. 22, no. 16, p. 6068, 2022.

[2] S. Singh, S. Chand, and B. Kumar, "Multilevel heterogeneous network model for wireless sensor networks," *Telecommun. Syst.*, vol. 64, pp. 259–277, Feb. 2017.

[3] G. Muhammad and M. S. Hossain, "A deep-learning-based edge-centric covid-19-like pandemic screening and diagnosis system within a B5G framework using blockchain," *IEEE Netw.*, vol. 35, no. 2, pp. 74–81, Mar./Apr. 2021.

[4] A. A. Barakabitze, A. Ahmad, R. Mijumbi, and A. Hines, "5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges," *Comput. Netw.*, vol. 167, Feb. 2020, Art. no. 106984.

[5] G. O. Boateng, G. Sun, D. A. Mensah, D. M. Doe, R. Ou, and G. Liu, "Consortium blockchain-based spectrum trading for network slicing in 5G RAN: A multi-agent deep reinforcement learning approach," *IEEE Trans. Mobile Comput.*, vol. 22, no. 10, pp. 5801–5815, Oct. 2023.

[6] S. S. Gill et al., "AI for next generation computing: Emerging trends and future directions," *Internet Things*, vol. 19, Aug. 2022, Art. no. 100514.

[7] A. R. Nandhakumar, A. Baranwal, P. Choudhary, M. Golec, and S. S. Gill, "EdgeAISim: A toolkit for simulation and modelling of AI models in edge computing environments," *Meas. Sens.*, vol. 31, Feb. 2024, Art. no. 100939.

[8] G. K. Walia, M. Kumar, and S. S. Gill, "AI-empowered fog/edge resource management for IoT applications: A comprehensive review, research challenges and future perspectives," *IEEE Commun. Surveys Tuts.*, vol. 26, no. 1, pp. 1–56, 4th Quart., 2023.

[9] M. Samaniego and R. Deters, "Internet of smart Things-IoST: Using blockchain and clips to make things autonomous," in *Proc. IEEE Int. Conf. Cogn. Comput. (ICCC)*, 2017, pp. 9–16.

[10] R. Singh and S. S. Gill, "Edge AI: A survey," *Internet Things Cyber-Phys. Syst.*, vol. 3, pp. 71–92, Mar. 2023.

[11] P. Fraga-Lamas, L. Ramos, V. Mondéjar-Guerra, and T. M. Fernández-Caramés, "A review on IoT deep learning UAV systems for autonomous obstacle detection and collision avoidance," *Remote Sens.*, vol. 11, no. 18, p. 2144, 2019.

[12] Y. Cui et al., "Deep learning for image and point cloud fusion in autonomous driving: A review," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 2, pp. 722–739, Feb. 2022.

[13] S. S. Gill et al., "Transformative effects of IoT, blockchain and artificial intelligence on cloud computing: Evolution, vision, trends and open challenges," *Internet Things*, vol. 8, Dec. 2019, Art. no. 100118.

[14] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for 5G and beyond networks: A state of the art survey," *J. Netw. Comput. Appl.*, vol. 166, Sep. 2020, Art. no. 102693.

[15] T. Tsourdinis, I. Chatzistefanidis, N. Makris, and T. Korakis, "AI-driven service-aware real-time slicing for beyond 5G networks," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, 2022, pp. 1–6.

[16] R. Kot, "Review of obstacle detection systems for collision avoidance of autonomous underwater vehicles tested in a real environment," *Electronics*, vol. 11, no. 21, p. 3615, 2022.

[17] A. Chakraborty, M. Kumar, and N. Chaurasia, "Secure framework for IoT applications using deep learning in fog computing," *J. Inf. Secur. Appl.*, vol. 77, Sep. 2023, Art. no. 103569.

[18] Y. Wu, Y. Ma, H.-N. Dai, and H. Wang, "Deep learning for privacy preservation in autonomous moving platforms enhanced 5G heterogeneous networks," *Comput. Netw.*, vol. 185, Feb. 2021, Art. no. 107743.

[19] Q. Zhang, H. Zhong, W. Shi, and L. Liu, "A trusted and collaborative framework for deep learning in IoT," *Comput. Netw.*, vol. 193, Jul. 2021, Art. no. 108055.

[20] B. Yin, H. Yin, Y. Wu, and Z. Jiang, "FDC: A secure federated deep learning mechanism for data collaborations in the Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6348–6359, Jul. 2020.

[21] I. A. Khan, N. Moustafa, D. Pi, W. Haider, B. Li, and A. Jolfaei, "An enhanced multi-stage deep learning framework for detecting malicious activities from autonomous vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 12, pp. 25469–25478, Dec. 2022.

[22] M. Wazid, A. K. Das, and S. Shetty, "BSFR-SH: Blockchain-enabled security framework against ransomware attacks for smart healthcare," *IEEE Trans. Consum. Electron.*, vol. 69, no. 1, pp. 18–28, Feb. 2023.

[23] H. Babbar, S. Rani, A. A. AlZubi, A. Singh, N. Nasser, and A. Ali, "Role of network slicing in software defined networking for 5G: Use cases and future directions," *IEEE Wireless Commun.*, vol. 29, no. 1, pp. 112–118, Feb. 2022.

[24] C. Ssengonzi, O. P. Kogeda, and T. O. Olwal, "A survey of deep reinforcement learning application in 5G and beyond network slicing and virtualization," *Array*, vol. 14, Jul. 2022, Art. no. 100142.

[25] D. Qian, S. Guo, L. Sun, Q. Hao, Y. Song, and M. Wang, "An integrity measurement scheme for containerized virtual network function," in *Proc. J. Phys. Conf. Ser.*, 2021, Art. no. 12029.

[26] E. Coronado, S. N. Khan, and R. Riggio, "5G-empower: A software-defined networking platform for 5G radio access networks," *IEEE Trans. Netw. Service Manag.*, vol. 16, no. 2, pp. 715–728, Jun. 2019.

[27] I. Gomez et al., "A software radio LTE network testbed for video quality of experience experimentation," in *Proc. 9th Int. Conf. Qual. Multimedia Exp. (QoMEX)*, 2017, pp. 1–3.

[28] C.-Y. Huang, C.-Y. Ho, N. Nikaein, and R.-G. Cheng, "Design and prototype of a virtualized 5G infrastructure supporting network slicing," in *Proc. IEEE 23rd Int. Conf. Digit. Signal Process. (DSP)*, 2018, pp. 1–5.

[29] C.-L. I, S. Kuklinskí, and T. Chen, "A perspective of o-ran integration with MEC, son, and network slicing in the 5G era," *IEEE Netw.*, vol. 34, no. 6, pp. 3–4, Nov./Dec. 2020.

[30] H. Grover, T. Alladi, V. Chamola, D. Singh, and K.-K. R. Choo, "Edge computing and deep learning enabled secure multitier network for Internet of Vehicles," *IEEE Internet Things J.*, vol. 8, no. 19, pp. 14787–14796, Oct. 2021.

[31] I. Mistry, S. Tanwar, S. Tyagi, and N. Kumar, "Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges," *Mech. Syst. Signal Process.*, vol. 135, Jan. 2020, Art. no. 106382.

[32] C. Feng et al., "Efficient and secure data sharing for 5G flying drones: A blockchain-enabled approach," *IEEE Netw.*, vol. 35, no. 1, pp. 130–137, Jan./Feb. 2021.

[33] S. K. Tayyaba et al., "5G vehicular network resource management for improving radio access through machine learning," *IEEE Access*, vol. 8, pp. 6792–6800, 2020.

[34] A. D. Dwivedi, R. Singh, K. Kaushik, R. R. Mukkamala, and W. S. Alnumay, "Blockchain and artificial intelligence for 5G-enabled Internet of Things: Challenges, opportunities, and solutions," *Trans. Emerg. Telecommun. Technol.*, p. e4329, Jul. 2021.

[35] H. Song, L. Liu, J. Ashdown, and Y. Yi, "A deep reinforcement learning framework for spectrum management in dynamic spectrum access," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11208–11218, Jul. 2021.

[36] M. Tahir, M. H. Habaebi, M. Dabbagh, A. Mughees, A. Ahad, and K. I. Ahmed, "A review on application of blockchain in 5G and beyond networks: Taxonomy, field-trials, challenges and opportunities," *IEEE Access*, vol. 8, pp. 115876–115904, 2020.

[37] T. Hewa, A. Braeken, M. Liyanage, and M. Ylianttila, "Fog computing and blockchain-based security service architecture for 5g Industrial IoT-enabled cloud manufacturing," *IEEE Trans. Ind. Informat.*, vol. 18, no. 10, pp. 7174–7185, Oct. 2022.

[38] X. Kong et al., "A federated learning-based license plate recognition scheme for 5G-enabled Internet of Vehicles," *IEEE Trans. Ind. Informat.*, vol. 17, no. 12, pp. 8523–8530, Dec. 2021.

[39] S. Yu, X. Chen, Z. Zhou, X. Gong, and D. Wu, "When deep reinforcement learning meets federated learning: Intelligent multitimescale resource management for multiaccess edge computing in 5G ultradense network," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2238–2251, Feb. 2021.

[40] B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell, "Bulletproofs: Short proofs for confidential transactions and more," in *Proc. IEEE Symp. Security Privacy (SP)*, 2018, pp. 315–334.

Authorized licensed use limited to: TIANJIN UNIVERSITY. Downloaded on April 30,2024 at 08:23:10 UTC from IEEE Xplore. Restrictions apply.