International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2024/36 Volume 11, Issue 5, September – October (2024)

RESEARCH ARTICLE

Multilayered Framework for Enhancing Data Confidentiality, Integrity, and Threat Detection through Blockchain, Advanced Cryptography, and Machine Learning

Rami Baazeem
Department of Management Information Systems, College of Business, University of Jeddah, Kingdom of Saudi Arabia (KSA)
✉ rbaazeem@uj.edu.sa

Received: 22 May 2024 / Revised: 06 August 2024 / Accepted: 23 September 2024 / Published: 30 October 2024

Abstract – Recent developments in the Internet of Things (IoT) have significantly expanded the interconnectedness of devices, leading to an increased need for strong security mechanisms. However, the proliferation of IoT networks has introduced critical vulnerabilities, particularly in data handling and storage, which are susceptible to unauthorized access, tampering, and malicious attacks. Addressing these challenges, this study proposes a multilayered Security Model for IoT that integrates advanced cryptographic techniques, blockchain technology, and machine learning algorithms to ensure the secrecy, integrity, and availability of data within IoT networks. The proposed model employs blockchain technology for decentralized, immutable data storage, effectively mitigating risks associated with unauthorized access and data tampering. Additionally, the model includes a deep learning-based malicious detection system, powered by a Convolutional Neural Network (CNN) in conjunction with the Q-Learning based Whale Optimization Algorithm (Q-WOA), to identify and counteract potential threats within the network. The result shows that the proposed CNN-Q-WOA models exceed others in most metrics. The proposed CNN-Q-WOA model excels accuracy with 0.965, which is higher than the others, leading to the higher overall correct prediction rate.

Index Terms – Data Confidentiality, Data Integrity, Threat Detection, Blockchain, Advanced Cryptography, Machine Learning.

1. INTRODUCTION

The expansion of the IoT gadgets have opened up a new era of connectivity and efficiency in daily life as they can easily talk with and exchange data among many smart tools. Although the proliferation of IoT does offer some advantages, there are still a lot of cybersecurity concerns especially as malware is concerned and security issues come to play [1]. Cyber-threats facing the IoT ecosystem has become progressively complex, as cybercriminals take advantage of device firmware vulnerabilities, unpatched internet protocols and cloud service loopholes to work with impunity. The traditional security strategies fade because they do not aptly deal with the constantly changing threats, thus the development of new strategies that use the power of the emerging technology [2] strive. The blockchain technology has shown to be a possible way to ensure that the networks IoT community have both security and credibility [3]. The blockchain, with its de-centralization of data storage and use of tamper-proof transaction mechanisms, will endow IoT environments with greater data privacy, authentication, and traceability. Besides, the immutable characteristic of Blockchains plays a essential role in the detection and monitoring of such incidents as cyber-attacks and unauthorized access [4]. In parallel with blockchain, metaheuristic algorithms and deep learning techniques handle the way malicious software can be detected and the threats identified in each sector of IoT ecosystem. Metaheuristic algorithms [5], like Particle Swarm Optimization (PSO) [6] and Genetic Algorithms (GA) [7], are aimed at improving various decision-making process and also tune parameters of malware detection algorithms, which leads to the evolution of malware detection algorithm. Utilizing deep learning methods, like Recurrent Neural Networks (RNNs) [8] and CNNs [9], which are based on large volumes of datasets, allow for pattern recognition (including in anomalous behavior) that is used to predict threats and to react accordingly. The mixture of blockchain with metaheuristic and deep learning algorithms is a synergetic approached bringing malware challenges down in IoT systems. Through the utilization of blockchain's decentralized and transparent nature and then incorporating the metaheuristic and deep learning algorithms' adaptive and self-learning abilities, organizations can build a robust front against various cyber threats considering a wide range of cyber-threats. Nevertheless, the future of a blockchain-based infrastructure for malware detection remains uncertain due to a number of

RESEARCH ARTICLE

crucial challenges such as a capacity limitation, inconsistency in integration and regulatory issues [10]. To overcome these impediments collaborative actions of academy, industry, and governance bodies are essential to elaborate new protocols, compatible frameworks and regulations which are favorable to the general encryption IoT systems implementation [11].

The IoT, is the next stage of the Internet development which brings new vulnerabilities, malware is the most prevailing threat. Data integrity could be spoiled, the devices themselves by the side of the line of target [12]. In an environment where traditional security mechanisms cannot handle the ever-changing nature of threats faster than elaborate resolutions are offered. Being bell-shaped, the IoT blockchain technology is beneficial to the IoT security by proposing the ledger, which is not subjected to centralization or a possibility of tampering [13]. Through employing blockchain, IoT structures which are now available to assure transparent, immutable ledgers for monitoring device activities as well as their abnormalities typically related to a malware presence. Among the algorithms that can assist blockchain in the identification of malware, metaheuristic and deep learning are the most effective. Metaheuristic algorithms support decision-making processes approaching optimum, while deep learning utilizes big data consequences for proactive identification [14]. Blockchain with advanced algorithms in the network creates a secure ecosystem for fighting off IoT malware threats and protecting critical information. This integration bears a far-reaching implication in the global enhancing of IoT security attachments [15].

As IoT devices has enabled never-seen-before connectivity, it has, however, brought major security gaps that can well be increasingly exploited by the malware threats [16]. The utilization of traditional security measures, however, doesn't contribute to the solution of some particular issues such as the limited resource and full of diversity among communication protocols in the IoT environments [17]. This poses threats such as cyberattacks from different malware viruses and thus impair data integrity as well as system security. including blockchain among the tools of IoT network disinfection may bring a solution to issues related to malware detection, as well as to security in general. Nevertheless, the main problems like interoperability and scalability should be resolved to turn a dream of collaboration of both of technologies into reality [18]. I would like to conduct research and design scalable frameworks that are capable of detecting threats associated with malware in IoT environment, using the capability of blockchain to ensure [software] security.

The purpose of conducting the study drives from the significant urgency of dealing with the current cybersecurity risks within the IoT system. With the increased micro-presence of IoT devices through the various industries and critical infrastructure, the threat landscape improves in both depth and width, and malware attacks become very grave as they pose a threat to data integrity, system security, and user privacy. The traditional solutions usually fail to account for the sophistication, diversity, and dynamic character of IoT malware security perils. Hence, the intelligent, sustainable development of IoTs systems is the key aspect to the question of their security. Blockchain technology presents a unique solution which is based on the characteristics that include decentralized, tamper- resistant data storage and transaction mechanisms. When blockchain technology is combined with the IoT frameworks, it becomes possible to create immutable and transparent ledgers to record devices' behavior in order to identify anomalies linked to a malware infection. The research questions we are going to answer in this research are as follows:

- How can the security of IoT networks, particularly in the context of routing attacks, be effectively enhanced?
- How can a multi-layered security model incorporating data validation, encryption, and intrusion detection be designed specifically for IoT routing?
- In what ways can cryptographic techniques like RSA encryption with SHA3-512 integrity verification address the security requirements of IoT data transmission?
- What is the efficiency and performance of the suggested security model in terms of resistance to routing attacks, as compared to existing models?
- In what manner does the proposed solution contribute to the broader discussions on the security of IoT network infrastructure beyond routing issues?

The objective of this research is to contribute to the ongoing discussions regarding the security risk of IoT networks, especially when routing attacks are targeting data integrity and the overall system security. The major contributions of the research paper include:

- This paper introduces a comprehensive multi-layered security model specifically tailored for IoT routing, addressing concerns related to routing attacks and emphasizing data integrity and system security.
- This study proposes a robust solution for data validation and encryption by employing RSA encryption with SHA3-512 integrity verification algorithm. This approach ensures secure data transmission within IoT networks, crucial for maintaining reliability and security.
- This study proposed a novel approach to cryptographic key generation using the TEO algorithm. This optimization outperforms traditional key generation methods, especially important in resource-limited IoT environments.

RESEARCH ARTICLE

- We have utilized Q-WOA algorithm to optimize the CNN hyper parameters, which is a crucial element in IoT security. Running simulations involving all the components of the proposed solution using Python to assess the efficiency of the solution.

The rest of the paper is structured as follows: A literature review that is of brief duration also determines the gaps that can be found among existing approaches is presented in Section 2. Proposed framework is provided and discussed in terms of architecture and blockchain, metaheuristic, and deep learning algorithm integration in Section 3. Experimental evaluation assesses outcomes and identifies indicators of output in section 4. Section 5 presents the discussion on the outcomes of this study with the limitations. Section 6 conclude the study with some future scope.

2. LITERATURE REVIEW

This literature review acts as a pivotal framework for comprehending the accumulated knowledge that is the foundation and background of the current research. The article takes the readers through an in-depth review of scholarly literature with an aim of providing a thorough analysis of the important theories, methodologies, and findings in the field. The literature review serves the purpose of not only revealing the areas of previous research with gaps and shortcomings but also enabling the formulation of the research questions and hypotheses based on the findings.

In this connection, the research [19] devises a machine learning based OMLIDS-PBIoT framework, a data driven intrusion detection system with the primary goal of protecting privacy in the smart city context. OMLIDS-PBIoT approach, provided with BC and ML methods, obtains security in the scope of smart cities. In this context, the process of data pre-processing is at the beginning where the OMLIDS-PBIoT approach converts it to a format that can be processed. Having mentioned that, FS model using GEO algorithm is also designed to reduce the number of features to prominent subsets. Another significant element of this intrusion detection system involved a RVFL model and a HBO based on a random vector network. Furthermore, blockchain technology ensures safe and secure data transfers when employed in the context of IoT-based smart cities. From the research findings, we can see that the OMLIDS-PBIoT is the best as compared with other techniques that are available at the present.

The study's author [20] suggests integrating blockchain technology into the system of monitoring as a tamper-proof method to ensure that security guidelines are adhered to even in the event that devices are compromised. The suggested solution, a blockchain-based architecture, differs from the current centralized and distributed security measures in that it considers the possibility that the solutions themselves could be affected. It is intended to list security regulations and only applies when a large number of devices are not harmed. The proposed architecture enables the seamless integration of current IoT devices through the use of add-on hardware modules and the permissioned blockchain (Hyperledger Fabric) and delivers noticeably less latency and overhead than permission-free blockchains (like Ethereum).

A secure image transmission and diagnostic model for the IoMT based on DL with blockchain support is presented in this research [21]. The model that is provided contains several processes such as data collecting, data security, hash value encryption, and data classification. In order to quickly generate the best ECC keys, elliptic curve cryptography (ECC) is essentially utilized in conjunction with the grasshopper with fruit fly optimization (GO-FFO) approach. Following that, the hash values are encrypted employing NIS-BWT, or neighborhood indexing sequences with burrow wheel transform (BWT). Ultimately, the classification process is used to a deep belief network (DBN) to ascertain whether a disease is present. To ascertain the analysis of the best outcomes of the model that is offered, a thorough experimental validation is conducted, and the outcomes are examined from a diversity of angles.

For the purpose of securing a multinational IIoT with offices spread across many nations, author have presented a hybrid Blockchain system in this paper [22]. Using a variety of security measures, the suggested architecture is thoroughly tested against traditional mechanisms. Our suggested method seems to achieve 94% efficiency when it comes to preventing DDoS and DoS threats, message modification attacks, and authentication delays, according to the simulation findings.

With the help of blockchain technology, the authors of this study [23] provide BASA, an efficient cross-domain IIoT safe device authentication method. Consort blockchain was developed specially to boost trust in a number of industries. The process of authentication entails the utilization of identity-based signatures, or IBS. We provide an identity management solution that may guarantee device anonymity in order to protect the privacy of devices undergoing authentication. Additionally, two sides agree on session keys, which may safeguard further conversations. Many experiments have shown the usefulness and efficiency of the suggested mechanism.

The study [24] offers a workable method for integrating FL with Blockchain technology to offer big data analytics services that are private and safe. Fuzzy hashing is a useful technique to identify variances and anomalies in FL-trained models, which can help to prevent poisoning attempts and guarantee the security of both user data and trained models. To model assault types and assess the suggested solution, a quasi-simulated environment is employed.

RESEARCH ARTICLE

Examining blockchain-based FL methods for complete IoT system security is the aim of this study [25]. It highlights the necessity of utilizing cutting-edge approaches for IoT ecosystem security and privacy by outlining the present state of blockchain research, how FL methods may use it, current IoT security challenges, and solutions. It also draws attention to open research problems and IoT data analytics from a security standpoint. There is also a comprehensive assessment of the literature on blockchain-based FL methods for IoT applications. In the end, this research addresses and considers the risks and challenges related to combining blockchain and FL in the IoT.

An overview of IoMTs is given in the study [26], which then explores their architecture. It then discusses how to transfer the current operations of the healthcare system into an architectural design. Furthermore, a number of cutting-edge technologies are expected to be essential in tackling a variety of e-healthcare challenges, like security, accuracy, privacy, and performance. These technologies include AI, SDN, Blockchain, and Physically Unclonable Functions (PUF). In conclusion, we provide three IoMT case studies: (1) Blockchain Assisted Patient Centric System; (2) AI-enabled SDN Assisted e-Healthcare; and (3) PUF-based Authentication, respectively. The techniques this study offers could have a big impact on how fast IoMT infrastructure can adapt to the evolving industry.

In a study [27], a two-layer malware spread-patch paradigm (IIPV) is proposed, accounting for the constrained central computer resources and rudimentary edge devices of the IoT. Its foundation is a patch distribution strategy that is hybrid. A differential game model was developed and the spread of malware in IIoT was fully investigated employing differential games. The optimal device control strategies for patches and viruses were then found by applying arbitrary effort factors to the optimization issue, which was further addressed utilizing optimization theory.

An analysis framework of an epidemic theory and individual-group game theory were the foundations of a novel viral spread model (STSIR) proposed by authors in a similar study [28]. By considering human behavior, this model more properly represents the spread viruses among gadgets. We modify and enhance the standard epidemic model SIR, focusing on the features of SIoTs, including limited social distance and dynamic number fluctuation of people and devices, to illustrate the kind of viruses that are consistently propagating to neighbor nodes.

Next, by building the attack and defense paradigm between vulnerable and impacted SIoT nodes utilizing an individual-group game, we address the dependence of infection and recovery rates on past experience. Ultimately, we employ a reward matrix to get the mixed Nash equilibrium solution.

The authors of the study [29] suggested edge computing-based IoT data sharing programs to use evolutionary security and privacy learning methodologies. We use evolutionary game theory to create a reward matrix that accurately depicts the intercommunication between edge nodes and IoT devices, as they are two sides in a game. To achieve their goal of acquiring personal data, IoT devices may pose malicious questions. Therefore, to avoid exposing IoT data, edge nodes should reject requests from rogue IoT devices. In the end, they maximize the gains by dynamically adjusting the plan to match the opponent's tactics.

According to the study [30], Deep Q-Network (DQN), which is defined as a discrete-time Markov decision process, handles the open-set identification issue in intrusion detection. In DQN's value network, a Conditional Variational Auto-Encoder is deployed concurrently. Therefore, the known traffic fine-grained classification difficulty and the unidentified assault recognition challenge are the two subproblems of the open-set recognition issue in intrusion detection. We use DQN to the well-known fine-grained traffic categorization issue. We utilize reconstruction error as a measure to detect unknown attacks since it is frequently lower for known traffic than it is for unknown assaults.

In a research, the Social IoT (SIoT) network traffic processing module creates samples of SIoT traffic, chooses samples to enter a cybersecurity examiner centre and a classifier, and outputs similarity [31]. The authors steadily enhanced a heuristic learning network's capacity to detect malicious traffic by integrating DQN into it. In particular, reward functions are created based on the network's chosen actions to penalize the inaccurate labelling of harmful samples and enable reward functions to be modified to accommodate varying execution actions. After that, to determine the best course of action for the heuristic learning network, the LSTM-based DQN maximizes the cumulative anticipated reward.

An IoT node's interactions with its associated edge node when operating an IoT resource-grant system are described in the paper by S. Shen et al. [32]. For privacy-preserving edge computing-based IoT networks, the study proposes a signaling game. Then, theoretically, we formulate the best privacy-preserving tactics for edge nodes. To solve the real-world issue of figuring out game parameters and convergent equilibrium, a signaling Q-learning approach is subsequently created. The theoretical results are validated by simulations based on two statistical points: the posterior chance of an IoT node being malicious and the ideal probability of an IoT node making a harmful request.

In order to increase the unpredictability of the detection approach, increase the detection rate given the presence of unknown malware families, and provide more effective detection without requiring constant detector upgrades to keep up with emerging spyware, the article [33] presented different

RESEARCH ARTICLE

ways to integrate both generic and specialized detectors in an effective manner during the analysis process. The study also suggests an alpha-count method that looks at how different detector combinations' speed and accuracy during malware analysis may be affected by the length of the observation time frame. Table 1 displays the overview of the literature review.

Table 1 Summary of the Literature Review

Ref.	Methodology Used	Results	Limitations
[19]	OMLIDS-PBIoT framework with BC and ML techniques; FS model using GEO algorithm; RVFL model and HBO based on a random vector network	Improved security in smart cities; OMLIDS-PBIoT outperforms other techniques	Limited discussion on resource requirements
[20]	A tamper-proof monitoring system based on blockchain technology; Permissioned blockchain (Hyperledger Fabric) with add-on hardware modules	Lower latency and overhead; Efficient prevention of DDoS and DoS threats	Evaluation limited to simulation findings
[21]	DL with blockchain assistance for protected image transfer and diagnostic model for IoMT; ECC with GO-FFO technique; NIS-BWT for HASH values encryption; DBN for classification	Optimized ECC keys; Thorough experimental validation; Disease classification accuracy examined	Limited discussion on scalability and real-world implementation
[22]	Hybrid Blockchain system for multinational IIoT security; Extensive testing against traditional mechanisms	94% efficiency in preventing DDoS, DoS threats, message modification attacks, and authentication delays	Limited details on specific security measures employed
[23]	BASA technique for cross-domain IIoT secure device verification; Consort blockchain with IBS; Negotiation of session keys	Effective cross-domain IIoT secure device verification; Anonymous device authentication; Session key negotiation	Limited discussion on the scalability of the proposed mechanism
[24]	Integration of Blockchain technology with FL; Fuzzy hashing for identifying differences and abnormalities in FL-trained models	Services for secure and confidential large data analytics; Attack mode simulation in a quasi-simulated environment	Limited discussion on the impact of various attack scenarios
[25]	Blockchain-based FL techniques for comprehensive IoT system security; Comprehensive survey of research; Examination of dangers and challenges	Contribution to IoT ecosystem security and privacy; Exploration of open research topics	Limited focus on specific FL techniques
[26]	Overview of IoMTs and architectural design; Integration of SDN, Blockchain, AI, and PUF	Case studies for IoMT based on Blockchain Assisted Patient Centric System, AI-enabled SDN Assisted e-healthcare, and PUF-based Authentication	Limited discussion on practical implementation challenges
[27]	IIPV paradigm for malware spread-patch based on differential games	Thorough examination of malware propagation in IIoT; Differential game model creation	Limited discussion on the adaptability of the proposed paradigm
[28]	Based on individual-group game theory, the STSIR viral spread model uses a reward matrix to solve a mixed Nash equilibrium.	Accurate representation of virus propagation in SIoTs; Individual-group game for attack and defense model	Limited exploration of diverse attack scenarios

RESEARCH ARTICLE

[29]	Evolutionary game theory for IoT data exchange strategy based on edge computing	Illustration of connectivity between edge nodes and IoT devices; Payoff maximization	Limited discussion on the adaptability of the proposed scheme
[30]	DQN for open-set identification in intrusion detection; Reconstruction error as a measure	Addressing open-set identification issue; Use of DQN in traffic categorization problem	Limited discussion on the generalization of the proposed approach
[31]	Traffic processing module for SIoT networks with heuristic learning network and DQN based on LSTM	Improved detection of malicious traffic; Integration of DQN into heuristic learning network	Limited details on the complexity and training requirements
[32]	Privacy-preservation signaling game, signaling Q-learning	Best privacy solutions, convergent equilibrium, simulation verification	Real-world variability, scalability issues, model accuracy dependence
[33]	Generic and specialized detectors, alpha-count technique	Unpredictability, enhanced detection rate, improved performance, observation time window impact	Validation needed, observation window dependence, computational overhead

The extensive review of literature within this study detects several key research gaps that underline the necessity for further investigation. While various frameworks and methodologies have been proposed to increase the privacy and security of IoT and IIoT systems, there remains a significant gap in addressing the scalability and real-world implementation challenges of these solutions. Many studies, such as those focusing on blockchain-based architectures and machine learning models, have demonstrated efficacy in simulated environments but lack comprehensive evaluation in diverse and dynamic real-world settings. There is a noticeable gap in the exploration of resource requirements and computational overhead associated with advanced security mechanisms. For instance, techniques involving deep learning and blockchain, though promising, often entail substantial computational demands, which are not adequately discussed or addressed in the current literature. The proposed system

The proposed study addresses several critical research gaps identified in the literature and contributes significantly to the field of IoT security. By developing a comprehensive and multi-layered security model specifically designed for IoT routing, this study tackles the issue of scalability and real-world implementation challenges. Unlike previous frameworks that demonstrated efficacy primarily in simulated environments, our approach has been rigorously tested through extensive simulations, ensuring its applicability in diverse and dynamic real-world settings.

3. MATERIALS AND METHODS

The 3-Layer Security Model for IoT is a comprehensive model that captures both the phases and the process of data handling at all stages as displayed in Figure 1. The blockchain technology is employed to the storage of data and is a decentralized, unchangeable and securely stored file system used to prevent unauthorized access and data tampering. Moreover, data decryption and encryption are essential elements of data security that are eliminated by the model using the RSA algorithm for cryptography. The RSA algorithm relies on having strong keys for data encryption. For this reason, the model combines the TEO algorithm, which improves efficiency and rises the security of the key management.

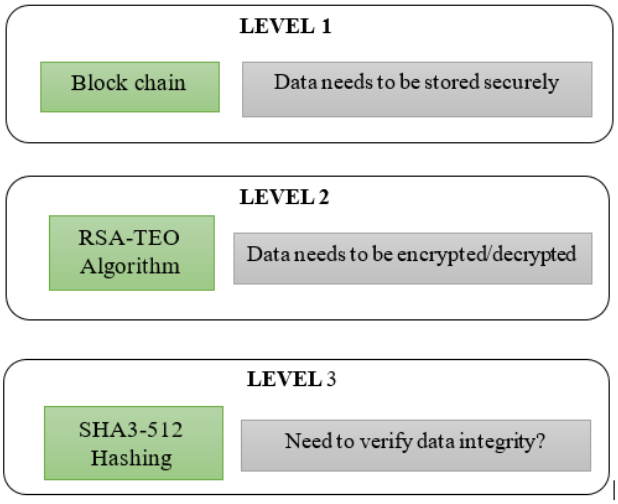


Figure 1 Overview of the Proposed 3-Layer Security Model for Internet of Things

The integrity of data is delicate, and therefore this in all cases uses the SHA3-512 hashing algorithm for data verification. This algorithm of a system of generation of a unique hash value for each batch of data is a high level of security which is very efficient as it makes it possible to detect any changes and corruption. Additionally, the scheme has the means to discover malicious behaviors within the network by a

RESEARCH ARTICLE

combination of advanced techniques. If there is any sign of suspicious activities, a deep learning-based malicious detection system powered by CNN with Q-WOA algorithm is applied. The integrated, more sophisticated approach is able to pinpoint the attacks and effectively fight them back, thus providing a full-blown security system for the IoT networks. The 3-Layer Security Model for IoT provides a multi-dimensional security architecture to protect data. The model essentially comprises of three levels of security aiming at confidentiality, integrity, and availability of information in IoT. All these three levels are described in detail in the subsequent sections.

3.1. RSA-TEO Based Data Encryption and Decryption

Rivest-Shamir-Adleman, or RSA, is a well-liked asymmetric encryption method that is frequently used to ensure the security of data transfer via networks. When the TEO algorithm is integrated, RSA experiences significant improvements in encryption and decryption capabilities, resulting in strengthened security and integrity of sensitive information. This integration introduces an innovative method to simplify key generation, encryption, and decryption processes, resulting in improved efficiency and security. During the encryption process, RSA key pairs are typically generated using well-established methods. Public and private keys make up these key pairs. The key generation process is improved to increase the strength and randomness of the keys with the incorporation of the TEO algorithm. TEO consistently fine-tunes the key generation process using thermal exchange principles, which boosts the randomness of the generated keys and strengthens their resistance against potential cryptographic attacks.

3.1.1. Thermal Exchange Optimization (TEO) Algorithm

The same as Newton's cooling rule, the TEO algorithm is an advanced metaheuristic optimization algorithm proposed in [34]. This law indicates that the rate of heat leaving a body relies not on the temperature variance between the body and its surroundings. In a process of heat transfer or thermal exchange there will be taking place the optimization between the cooling item and the environment. The potential new temperature for the object after its falling is also being considered as a new location in the search area. The algorithm employs this thermal conversation process to continually change the position of the warming object in an investigation to find a better solution. By borrowing principles from various disciplines, we can create powerful tools that can solve complex real-world problems efficiently. A detailed description of the TEO algorithm is given below:

Step 1: Initialization

Assign initial temperatures to all objects in a search space. This is done using the equation (1).

$$\mathrm{TEMP}_{0i} = \mathrm{TEMP}_{\min} + r_1 \times (\mathrm{TEMP}_{\max} - \mathrm{TEMP}_{\min}) \quad (1)$$

Where, TEMP_{0i} is the preliminary resultant vector of the i^{th} object, $\mathrm{TEMP}_{\min}$ and $\mathrm{TEMP}_{\max}$ are the lower and upper bounds of the design variables, and r_1 is a random vector with every element between 0 and 1.

Step 2: Evaluation

Calculate the cost value of every object with the method of objective function.

Step 3: Saving

To realize a high-performance algorithm and at the same time keep the computing costs low, the idea is to implement a Thermal Memory (TM) that stores the optimal solution found so far. Through this mechanism, the algorithm can quickly select and reuse the most appropriate existing solution, sparing the need for fundamental calculations. The implementation of the TM is effected through a process in which a number of worst performing individuals of the population are replaced through feeding the optimal solution from the TM.

Step 4: Creating groups

The agents should be paired based on a predetermined pattern after splitting them into two same-size groups. The pairing pattern is mostly set by the algorithm creator, and it can change, depending on the problem being addressed by the algorithm. For example, in some circumstances, agents are assigned randomly, whereas in others, an affinity or dissimilar match is used. The agents shall exchange the information and subsequently use the information from their partner to identify the objective function.

Step 5: Defining β

The TEO algorithm Step 5 employs the beta value rule for each object in the search space. This stage means a factor determining the cost or fitness value of the objects to be assigned differently among objects that have higher costs and belong to the lower weights group and objects that have lower costs and belong to the higher weights group.

Equation (2) used to calculate β for every object is:

$$\beta = \frac{\mathrm{Cost}_{\mathrm{object}}}{\mathrm{Cost}_{\mathrm{worst\ object}}} \quad (2)$$

where $\mathrm{Cost}_{\mathrm{worst\ object}}$ is the value or fitness cost of the worst object in the search space and $\mathrm{Cost}_{\mathrm{object}}$ is the cost or fitness value of the current object being evaluated. The item with the greatest cost or fitness value in the current population or iteration is considered to be the worst. Statistically, the probability of an item to be used for heat exchanging with other object, is proportional to. Such items are more likely to

RESEARCH ARTICLE

be the exchange offer than are less important ones, and the other way around too.

Step 6: Defining t

Throughout the search phase, the parameter t is utilised to stabilize out exploration and exploitation. To direct the algorithm toward better answers, a dynamic parameter varies with the number of iterations. Using equation (3), step 6 entails determining the value of t for each agent:

$$t = \frac{\text{iteration}}{\text{Max iteration}} \quad (3)$$

Where iteration is the current iteration's integer and Max iteration denotes the amount of iterations that may be performed. The initial value of t is modest, which encourages exploration of the search space to uncover potential solutions. As the algorithm develops, the value of t rises, progressively shifting the emphasis toward the utilization of the thus far discovered potential solutions.

Step 7: Escaping from local optima (i)

The next step in the optimization process involves adjusting the environmental temperature to avoid the agents from getting stuck in local optima. Local optima refer to solutions that may appear optimal within a certain range, but are not the global optimum. When agents get stuck in a local optimum, they may continue to search for solutions in that area, unable to escape and explore other potentially better solutions in the search space. To avoid this, the environmental temperature is adjusted using equation (4) that takes into account the current temperature, the iteration number, and a cooling rate.

$$\text{TEMP}_{\text{environment}}^{\text{Modified}} = \left(1 - \left(c_1 - c_2 \times (1 - t)\right) \times r_2\right) \times \text{TEMP}_{\text{environment}}^{\text{Previous}} \quad (4)$$

where c_1 and c_2 are controlling variables. $\text{TEMP}_i^{\text{Modified}}$ is the modified object's temperature and $\text{TEMP}_i^{\text{Previous}}$ is the previous temperature of object.

Step 8: Updating the agents

Step 8 of the algorithm involves updating the temperature of each object in the system. Equation (5) used to update the temperature of each object is:

$$\text{TEMP}_i^{\text{new}} = \text{TEMP}_{\text{environment}}^{\text{Modified}} + \left(\text{TEMP}_i^{\text{old}} - \text{TEMP}_{\text{environment}}^{\text{Modified}}\right) \times \exp(-\beta t) \quad (5)$$

Where, $\text{TEMP}_i^{\text{new}}$ is the new ith object's temperature, $\text{TEMP}_i^{\text{old}}$ is the old temperature of the ith object, $\text{TEMP}_{\text{environment}}^{\text{Modified}}$ is the temperature of the environment surrounding the ith object, β is a parameter that controls the rate of temperature alteration, t is the time step of the simulation

Essentially, this formula is updating the temperature of each object based on its previous temperature, the temperature of its environment, and the amount of time that has passed since the last update. The exponential term in the formula, $\exp(-\beta t)$, represents the rate at which the temperature of the object changes. As t increases, the term becomes smaller, which means that the temperature change rate reduces over time. The β parameter controls how quickly the temperature change rate reduces. A larger value of β means that the temperature change will decrease more quickly over time.

Step 9: Leaving from local optima (ii)

Introduce the parameter Pro, which is a number between 0 and 1 that determines whether an element of every cooling object necessity be altered or not. If $\text{Ran}(i) < \text{Pro}$, where $\text{Ran}(i)$ is a arbitrary number between 0 and 1, change one dimension of the i^{th} agent using Equation (6):

$$\text{TEMP}_{i,j} = \text{TEMP}_{j,\min} + r_3 \times \left(\text{TEMP}_{j,\max} - \text{TEMP}_{j,\min}\right) \quad (6)$$

Step 10: Checking terminating conditions

After a fixed of iterations, stop the optimization method. Return to Step 2 for a fresh iteration if the condition is not met. Stop the process and provide the finest results discovered if the criterion is met.

3.2. Data Integrity

The RSA key is responsible for encrypting the data and obtaining the hash in addition to the data itself from the blockchain. This information will be obtained by hackers or anybody else who does not have authorization to access the data, particularly via a man-in-the-middle assault. In order to ensure that the message is not tampered with, it is first hashed, then encrypted using the sender's private key, then concatenated with the plaintext version of the message, and lastly encrypted using a symmetric key. At the receiver's end, when the transmission has been decoded, it is separated into plaintext messages and encrypted hashed messages. A public key belonging to the sender is used by the receiver in order to decode the encrypted hashed message. This same public key is also utilized in order to hash the plaintext message. The integrity of the message may be verified by comparing the two hashes that were created. As a result, RSA with a key based on TEO is very safe when using the SHA3-512 algorithm. Furthermore, as was previously mentioned, the hashed key is stored on the Blockchain with the ciphertext. Following then, the process of decryption involves transforming the ciphertext into the original text.

3.3. Decryption Algorithm

Within the IoT, decryption is used to reverse the process of encryption and retrieve the original plaintext data from the ciphertext. This is done in order to ensure the safety of data that is transferred across IoT devices and other mechanisms

RESEARCH ARTICLE

that are part of the IoT ecosystem. The process of decryption often involves the use of a decryption key that is only known to authorized individuals. This is done in order to facilitate the process of restoring the ciphertext to its initial position. This key must be kept confidential and secure in order to prevent unauthorized individuals from gaining access to the content that has not been encrypted. The first data block is recovered from the created key itself during the decryption process. The SHA3-512 hash calculation is then applied to the subsequent block once the first block has been retrieved. For the very first time, the CNN-Q-WOA has been used to activate the third level of protection. In light of this, the encrypted Internet of Things data is subjected to further analysis and discussion in the following section.

3.4. Proposed Intrusion Detection System

For the purpose of identifying harmful assaults on the Internet of Things network, approaches based on deep learning are deployed. To determine the kind of traffic that is present on the Internet of Things network, our suggested model employs a traffic categorization approach that is based on routing. After that, a CNN-Q-WOA protocol is applied to the stream in order to identify any potentially malicious activity.

As shown in Figure 2, The scheme of IDS with CNN and Q-WOA starts by pre-treating network traffic data, cleansing and normalizing it. The TEO system is used to get the features relevant for this task. The DNN architecture design is done and the optimized hyperparameters are achieved with the help of Q-WOA. The CNN is trained by forward and back propagation, and its activation function is dependent on PReLU while Adam optimizer is employed. The issue of Q-learning is established by describing states, actions, rewards, and Q-values. The Q-matrix is initialized first, and then a whale population is produced, each of the whales representing a different CNN architecture. The best whale fit is selected upon CNN model performance indicators; the selected whale then is given the title of the best whale ever. Whale location and speed are updated with peripheral prey and bubble net attacking motion. The Q-learning is used to modify the Q-values, and, after that, the algorithm sets the stopping conditions and goes for the selection of the final best whale. The last CNN is trained, and another flow of the network traffic data is categorized as normal or breach.

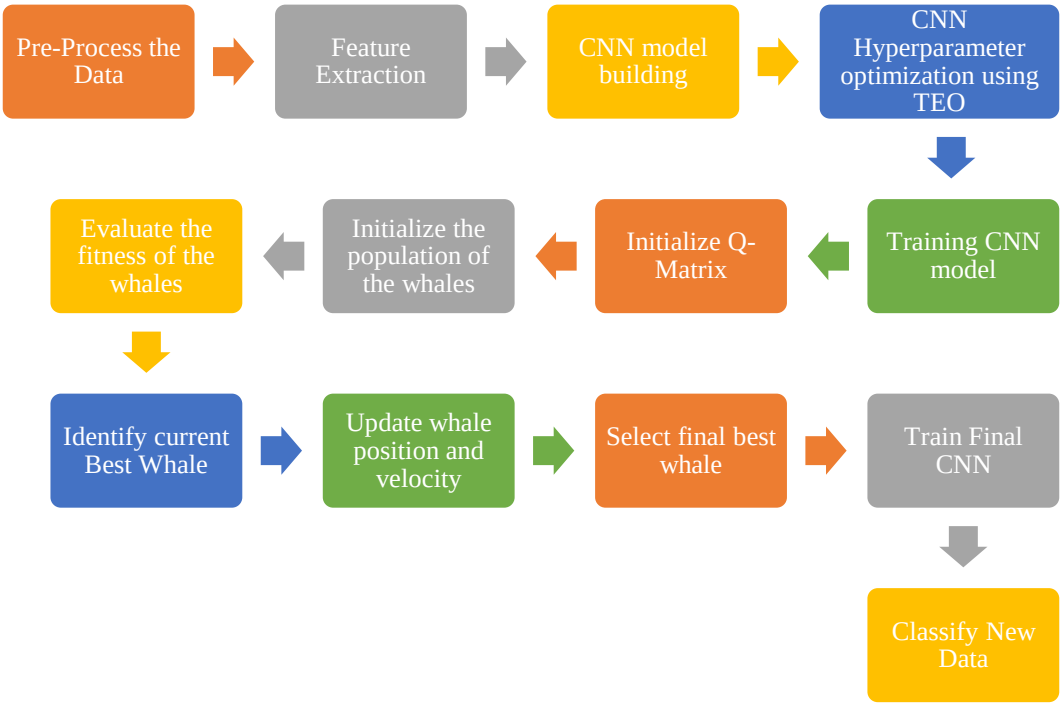


Figure 2 Overview of the Proposed Intrusion Detection and Classification Algorithm

Following are the procedures that taken in order to do malicious detection:

3.5. Data Pre-Processing

After collecting the data, the pre-processing method is called. The pre-processing turns the data into a good dataset. The data preprocessing is an outcome of data cleaning, and the use of data normalization techniques. We might calculate that the data was plentiful in duplicate records, incomplete data, or were noisy it. Consequently, the data was split into the features which were individual sets of values to make sure that the features lacked any blank values or mistakes in them.

RESEARCH ARTICLE

The missing values were replaced by averages that were used to ensure the quality of the data. This step enables us to ascertain that the data had gone through complete cleaning and preparation ideally required for analysis. It is possible for the numerical data to be created in a variety of ways, and the means or variances of these factors may be the source of problems in studying, as well as the potential to undermine the efficiency and precision of learning techniques. The z-score transformation was used in order to solve this issue. This was done in order to reduce the impact of outliers, which had a negative impact, by translating all of the data points into a standardized range that ranged from zero to one. In addition, the transfer of the preprocessed data into the feature extraction is carried out at this step.

3.6. Feature Engineering

In this study, the feature engineering process is meticulously designed to extract meaningful information from the pre-processed data, ensuring that the resulting features are both relevant and informative for the subsequent analysis. It is the weighted entropy variance that is used for the purpose of projecting feature selection. The equation for it is as follows: (7).

$$E = -\sum_{k=1}^{G} W_k . P_k . log \frac{P_k}{\sigma_k^2} \quad (7)$$

Here, W_k represents the weight assigned to each feature value, and P_k represents the probability of occurrence of each feature value. A TEO method is used to get the features that have been extracted, especially the Weighted Entropy and Variance components.

3.7. Attack Classification Algorithm

A CNN that has been optimized is used to choose the features, and then those features are classed for the intrusion. Utilizing the Q-WOA Algorithm, the CNN has been optimized. In addition, the accuracy of the prediction made by the malicious attack detection model may be improved by fine-tuning the activation function of the CNN with the use of the Q-WOA algorithm. The result that is the result of the hybrid classifier will be the result that is discovered.

3.7.1. CNN Model Architecture

The DL model being proposed incorporates a CNN along with a standardized multi-layer perceptron, as an alternative to a fully connected FNN. In contrast to FNN, CNN employs convolution as a mathematical operation in lieu of multiplication [35]. The process of convolution encompasses the utilization of custom hyperparameters, including the dimensions of the filter, the number of filters, and the strides, which are employed to generate the resulting matrix. In order to address the issue of diminishing tensor dimensions during the propagation of input through multiple convolutional layers, the technique of input padding was introduced. In this case, the pooling layer is employed to lessen or down sample the dimensions of the features within the layers by operating between successive convolutional layers. Subsequently, a fully connected layer incorporating regularization is observed, which is then succeeded by the classification output layer.

3.7.2. Forward Propagation

The objective of forward propagation is to make predictions, specifically to distinguish between attack and normal outcomes, through the utilization of CNN. The utilization of a multi-layer perceptron is a common approach in the implementation of ANN, which serve as the foundation for deep neural networks. The primary equation of the perceptron is denoted as equation (8):

$$y = \sum_{i=1}^{n} x_i w_i + b \quad (8)$$

Here, the variable n denotes the quantity of nodes present in a specific layer. The variable x denotes the values associated with these nodes, which correspond to the values of the dataset being analysed. The w_i denotes the weights assigned to the links between nodes, indicating the strength of these connections. Lastly, b denotes the constant value bias associated with the nodes in the layer. The obtained outcomes will be given into activation functions.

Additionally, this constraint restricts the outcomes to a finite scope. The activation functions commonly utilized in neural networks include Sigmoid, tanh, REL, LReLU, ELU, SoftMax, and PRelu. In this particular model, PreLU activation function was employed in the hidden layers shown by equation (9).

$$f(y_i) = \begin{cases} y_i, & if\ y_i > 0 \\ a_i * y_i & if\ y_i \leq 0 \end{cases} \quad (9)$$

Where, y_i represents the output of the activation function, f, for a given input y_i. The y_i is denotes the input to the activation function. a_i is considered as learning parameter and is dynamic in nature that change based on the activation function. It solves problem of ReLU and LReLU as

- If a_i = 0 f act as ReLU.
- If a_i > 0 f act as LReLU.
- If a_i = learning parameter then f act as PReLU

3.7.3. Back Propagation

Backpropagation is a commonly utilized method for training deep neural networks through the adjustment of weights and biases. The subject matter encompasses both loss functions and optimizers. To get the best values for the neural network, the loss function—also called the cost function—is used to minimize the value. A cost function, which is sometimes referred to as a loss function, can be used to evaluate the model. The minimization of the loss function will serve as the

RESEARCH ARTICLE

guiding principle for determining the optimal value of each parameter. The loss is calculated by equation (10).

$$loss = \frac{1}{2}(|y - \hat{y}|)^2 \quad (10)$$

Cross entropy is a concept commonly used in the field of information theory and ML. It measures the average number of bits needed to the utilization of loss functions. For a perfect IDS the loss should be minimum. Some of the most frequently encountered Loss Functions include Batch gradient descent, SGD, SGD with momentum, RMSprop, Adagrad and Adam. Based on the results obtained from testing multiple optimizers, it was determined that Adam performed the best. Equation (11) is a basic equation to calculate the new weight while moving backward and n is the learning rate.

$$W_{new} = W_{old} - n * \frac{\partial L}{\partial W_{old}} \quad (11)$$

Here, W_{new} represents the new weight value obtained in the optimization process. W_{old} on the other hand, denotes the previous weight value before optimization. The variable n stands for the learning rate, a critical parameter governing the size of steps taken during gradient descent, a fundamental optimization technique in machine learning. Additionally, $\frac{\partial L}{\partial W_{old}}$ represents the partial derivative of the loss function L with respect to the old weight W_{old}. This derivative guides the optimization process by indicating the rate of change of the loss concerning the weight.

The utilization of Batch Normalization was implemented to layers of CNN in order to mitigate the problem of overfitting and enhance the efficiency of the deep neural network model. A dropout (0.01) procedure involves the random removal of neurons along with their corresponding connections. The He init is used to initialize the weight in case of normal and uniform through equation (12), (13), and (14).

$$W_{i,j} \cong u(-\sqrt{\frac{6}{fan\_in}}, \sqrt{\frac{6}{fan\_out}}) \quad (12)$$

$$W_{i,j} \cong N(0, \sigma) \quad (13)$$

$$\sigma = \sqrt{\frac{2}{fan\_in}} \quad (14)$$

Where, $W_{i,j}$ represents the weight value located at position (i, j) within the weight matrix. This weight value is crucial as it determines the strength of connections between neurons in the neural network. Next, the variables u and N denote the types of distributions used for weight initialization, with u representing the uniform distribution and N representing the normal distribution. The variable σ stands for the standard deviation, which is utilized for initializing weights in the normal distribution. It influences the spread or dispersion of weight values around their mean during initialization. Additionally, fan_in and fan_out characterize the number of input and output units, respectively, for a particular layer in the neural network.

3.8. Q- Learning

Q-learning is a ML approach that is utilized for solving RL problems [36]. In reinforcement learning, an agent learns how to engage with an environment by taking actions and receiving rewards. The goal of the agents is to get the most out of the cumulative reward with time by learning which actions lead to the most significant rewards. A modelling of the environment is not necessary for the model-free RL method known as Q-learning to function. Instead, it employs a table of Q-values, which indicate the anticipated future rewards for taking a specific action in a particular state. When the agent interacts with the surroundings, the Q-values are gradually adjusted, balancing exploration and exploitation that used a learning rate and a discount factor.

The mathematical equation for Q-learning is presented in Equation (15):

$$Q(s,a) = Q(s,a) + \alpha \times (R(s,a) + \gamma \times max(Q(s',a')) - Q(s,a)) \quad (15)$$

Here, $Q(s,a)$ denotes the Q-value for a state-action pair (s,a), α denotes the learning rate, γ denotes the discount factor, $R(s,a)$ denotes the reward for performing action a while in state s, $max(Q(s',a'))$ is the maximum Q-value for the subsequent state s' and all feasible actions a'.

3.9. The Proposed Q-WOA Algorithm

WOA is an algorithm that admires nature and applies the way humpback whales hunt. It works on the similar principle of the humpback whales who find their prey after following the signals. The algorithm is described by Mirjalili et al. in 2016 and has been applied in various optimization problems [37]. WOA is an algorithm that tells make of symulating the search algorithm of humpback whales. The algorithm is divided into three sections: encircling, spiral, and search.

A hybrid Q-WOA method which is based on Q-learning and WOA is used intrusion detection system. The WOA algorithm is trying to find the best solution from the search space. At the same time the Q-learning algorithm is updating the Q-matrix which consist of the predicted rewards for each state-action combination. Here are the steps for the Q-WOA based intrusion detection system:

3.9.1. Define the Q-Learning Problem

The stages, goals, rewards, and the Q-values for the Q-learning formulation for scheduling job workload in a cloud service system are stipulated in this step. Manner of state means the current state of the cloud, which states about the way attacks needed to be detected. The action is understood as decision making of attacks in intrusion detection system.

RESEARCH ARTICLE

Reward is the aggregate of all the objectives, which can be measured along these objective functions such as makespan, energy consumption and so on. The Q-value is the provides predicted future reward of a state-action pair, which would be set to zero initially.

3.9.2. Q-Matrix Initialization

Initialize the Q-matrix with initial Q values for all the state-action combinations, which are present in initial state. The Q-matrix is analogous to a table row by states column by actions. The table serves each condition with the predicted reward of a state-action pair.

3.9.3. Generate the Initial Whale Population

In the Q-WOA algorithm, we first create the whale initial population with just some of its members randomly located in space and speed. Whale position is a place of a solution to a problem while the speed of it movement reflects the velocity direction and speed of navigation in a search space.

3.9.4. Evaluate the Fitness of the Whales

Compute the fitness of every whale in the population using the multi-objective function. An assessment is either a good solution to a problem when it has multiple objectives and constraints or it is not.

3.9.5. Set the Current Best Whale

Select the best whale from the current population as the current best whale. The best whale is the one with the highest fitness value. This step is important as it helps to keep track of the finest resolution establish so far and guide the search towards better solutions in subsequent iterations.

3.9.6. Update the Position and Velocity of the Whales

The update of position and velocity is performed by employing the encircling prey and bubble net attacking approach of humpback whale. As explained below

In the encircling phase, the whales surround a prey and move towards it. This phase is represented by a linear decrease in the search space around the best result found so far. The whales use a strategy called "bubble net" to encircle their prey, which involves creating a bubble net around the prey to prevent it from escaping.

$$\vec{D} = \left|\vec{C} \times \vec{X}^*(t) - X(t)\right| \quad (16)$$

Equation (16) calculates the displacement vector $\vec{D}$, which represents the distance between the current position of the whales $X(t)$ and the position of the best solution found so far $\vec{X}^*(t)$. The $\vec{C}$ represents a randomly generated vector.

$$\vec{X}(t+1) = \vec{X}^*(t) - \vec{A} \times \vec{D} \quad (17)$$

Equation (17) then updates the position of the whales for the next iteration $\vec{X}(t+1)$. It does so by subtracting from the current position $\vec{X}^*(t)$ a scaled version of the displacement vector $\vec{D}$, where $\vec{A}$ represents a randomly generated vector of scaling factors.

After the best search agent has been found, the other search agents will make an effort to move closer to that agent. These equations serve as examples of this phenomenon:

3.9.7. Perform the Q-Learning Update

Now, we utilise the Q-learning update rule to update the Q-matrix. The Bellman equation as shown in Equation (18), on which the Q-learning update rule is founded, determines the revised Q-value for a state-action combination using the present Q-value and the immediate reward.

$$Q(s,a) = Q(s,a) + \alpha \times (R(s,a) + \gamma \times max(Q(s',a')) - Q(s,a)) \quad (18)$$

Here, $Q(s,a)$ signifies the Q-value for a state-action pair (s,a), α is the learning rate, γ is the discount factor, $R(s,a)$ is the reward for taking action a in state s, $max(Q(s',a'))$ is the maximum Q-value for the next state s' and all probable actions a', and s and a are the current state and action, respectively.

3.9.8. Check the Stopping Criteria

Verify that the stopping requirements, such as the algorithm's convergence or the maximum number of iterations, are fulfilled. Till the stopping requirements are satisfied, repeat steps 4 through 8. Select the final best whale: Select the best whale from the final population as the final best whale.

3.9.9. Output

Once the algorithm has completed its execution and identified a set of ideal solutions, the next step is to evaluate the quality of each solution using the multi-objective function and constraints of the delinquent.

The evaluation of the solutions involves measuring the performance of each solution based on the specified objective functions and constraints. After evaluating the quality of each solution, the final step is to output the best solution or set of solutions that satisfy the optimization criteria. This step involves selecting the solution or set of solutions that perform the best in terms of the specified objective functions and constraints.

4. EXPERIMENTATION

Here, we conducted the elaborated experimental framework to determine the robustness and efficiency of the suggested federated learning based IoT framework for malware identification.

RESEARCH ARTICLE

4.1. Experimental Setup

In order to shed light on generation time of the encryption key, decryption time, response time when sharing records, freezing time, as well as learning rates that 75% and 90% in blockchain security, we conducted the investigation. The implemented metrics were chosen with precision in order to observe the working of the suggested architecture in a scenario where IoT technology is coupled with blockchain support. We aimed to evaluate how the security and overall efficiency of the system were influenced by different learning speeds that was very beneficial for our future investigation because it makes the system more resilient and adaptable under a variety of operating conditions. An extensive comparison between the advanced RSA-TEO protocol and the traditional key generation techniques were carried out. The conventional algorithm which contains the random number generation (RNG) [38] that depends on creating the random numbers for keys and Diffie–Hellman key exchange (DHKE) [39] that is the symmetric key exchange algorithm to create the secure keys for an untrusted communication channel is being evaluated now. Consequently, we considered shifting to the RSA algorithm [40] which is one of the most popular encrypted methods ever that has been used as the base criteria for many cryptographic applications. The main purpose of this comparative research is to assess the performance and efficiency of the new RSA-TEO algorithm in comparison with the already existing algorithms, giving consideration to the key generation efficiency, security, and being suitable for different cryptographic scenarios.

Table 2 Simulation Parameters

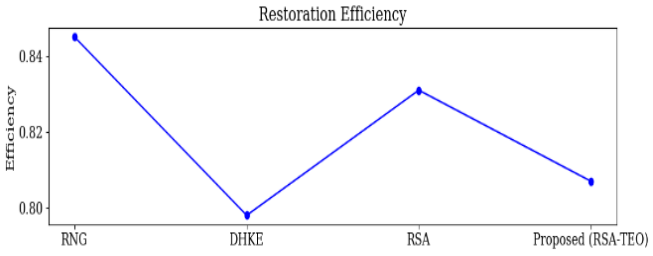
	Parameters	Values
1.	Number of neurons in Output layer	5
2.	Number of neurons in Input layer	41
3.	Optimization Function	Adam Optimizer
4.	Normalization	Batch Normalization
5.	Weight Initialization	He init
6.	Activation Function in Hidden layer	Parametrized ReLU
7.	Activation Function in Outer layer	Multiclass SVM
8.	Learning rate	0.01-0.5
9.	Dropout rate	0.01
10	Numbers of Epoch	50

In the Table 2, which contains the simulation parameters, the main constituents are specified in order to set up the model of neural network. The 41 neurons are assigned to the input layer, whereas the 5 neurons constitute the output layer. The loss minimization function used for training the model is Adam Optimizer, which is a very efficient technique of optimizing stochastic objective function. In order to improve training, the batch normalization is being used for normalization features. The weight initialization is conducted using the He initialization technique. This method is applicable for deep neural networks. The second layer, the hidden layer, is instantiated using the parametrized ReLU as the activation function, which contributes to the model's non-linearity. Learning rate is put between 0.01 and 0.5, this is a parameter in optimization and dropout rate of 0.01 is implemented to avoid overfitting. The model undergoes training for a variable number of epochs, which is between 25 and 400, so that the weights in the neural network adapt and refine with the successive iterations to achieve the best performance. The ones being defined are the ones that guide the model in the simulation, including its configuration and training parameters.

MTTD (Mean time to detection) is actually the first and the most important metric in system monitoring as well as in the context of responding and solving problems when an event happens. This metric provides a quantitative measure of the average period of time suitable for a system or a mechanism like intrusion detection to identify and detect the event which have already occurred.

4.2. Dataset

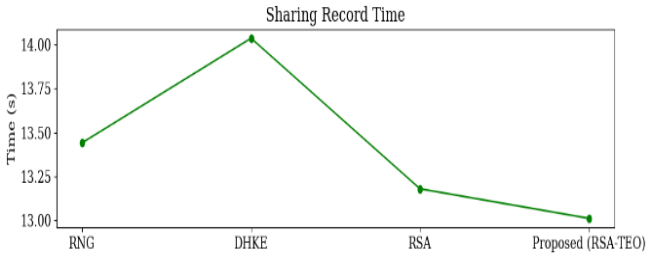
The NF-UQ-NIDS dataset [41] is intended to be used by researchers to train and assess the performance of IDS which are based on machine learning techniques using University of Queensland (UQ) network traffic data. These bulletproof recon sets are a comprehensive set of 11 million entries in a user-friendly CSV format. This collection is over 77% traffic that can be considered benign and 23% of all traffic includes various attack mechanisms. These attacks are variably from DoS, U2R to information gathering and brute-force attacks. The dataset is merged which is considered to be its main strong point.



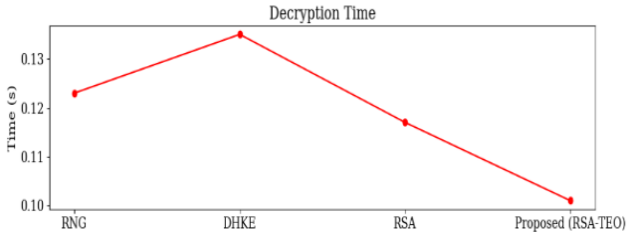
(a) Restoration Efficiency

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2024/36 Volume 11, Issue 5, September – October (2024)

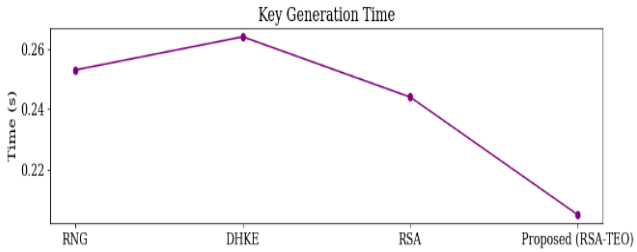
RESEARCH ARTICLE



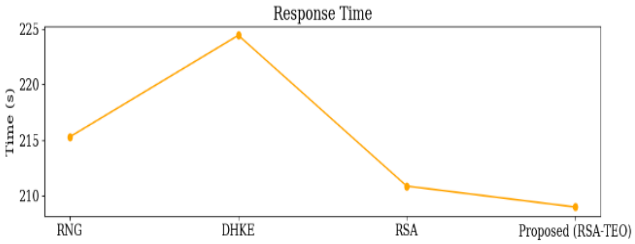
(b) Sharing Record Time



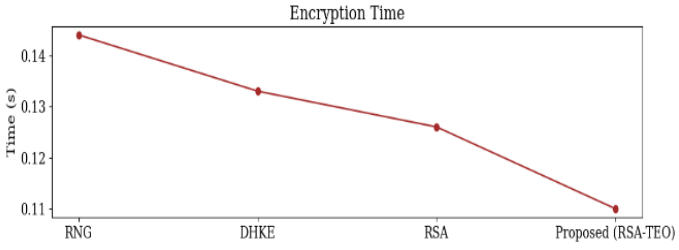
(c) Decryption Time



(d) Key Generation Time



(e) Response Time

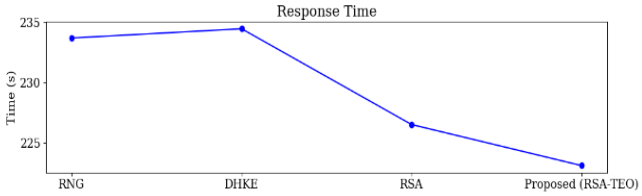


(f) Encryption Time

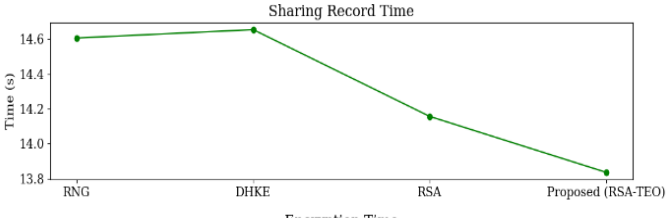
Figure 3 Evaluation of Performance Metrics at a 75% Learning Rate

4.3. Results

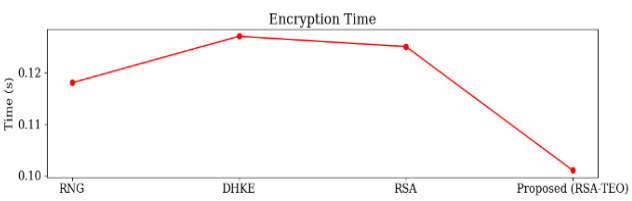
Table 3 and Figure 3 results summarize the performance time of the suggested RSA-TEO algorithm comparing against the traditional algorithms—RNG, DHKE, and traditional RSA. With learning rate of 75%, the proposed method demonstrates the consistent best results across several key metrics. The efficiency of the suggested RSA-TEO in the context of encryption time is demonstrated by its faster performance than RNG, DHKE, and traditional RSA, resulting in significant amount of seconds saved for encrypting the data. On the other hand, RSA-TEO's decryption time is strongly improved as well, making them much faster in comparison to other algorithms. This efficiency is really shown in the response time metric where the proposed RSA-TEO gets a smaller response time which means a quicker and a more responsive system. Key generation time is one of the crucial factors in cryptographic algorithms. The new RSA-TEO algorithm performs better at this point than the RNG, DHKE, or the traditional RSA algorithm. RSA-TEO key generation is greatly effective, easier and more rapid by making it as streamlined as possible. System's recovery and restoration ability among others is what makes restoration efficiency, a key indicator of the system's ability to recover and restore, prominent in the proposed RSA-TEO algorithm. This means that the method proposed not only excellently performs encryption and decryption, but it is also resilient to data restoration which achieves better results than RNG, DHKE, and classical RSA.



(a) Response Time

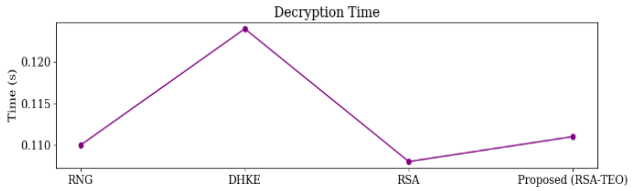


(b) Sharing Record Time

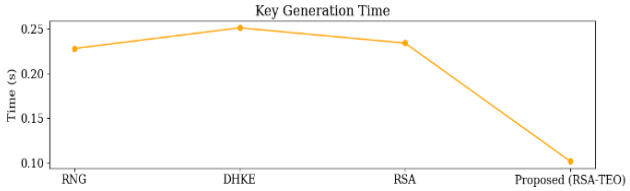


(c) Encryption Time

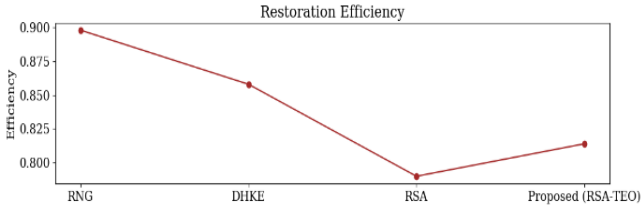
RESEARCH ARTICLE



(d) Decryption Time



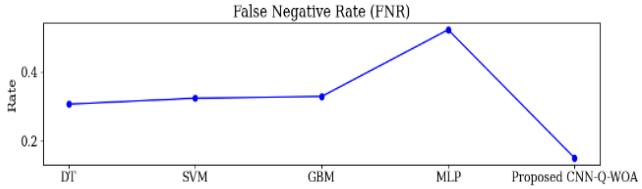
(e) Key Generation Time



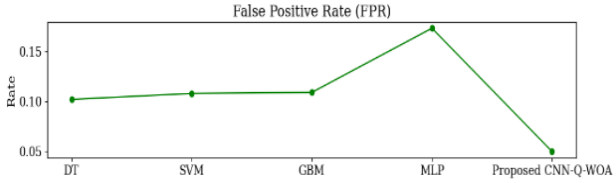
(f) Restoration Efficiency

Figure 4 Evaluation of Performance Metrics at a 90% Learning Rate

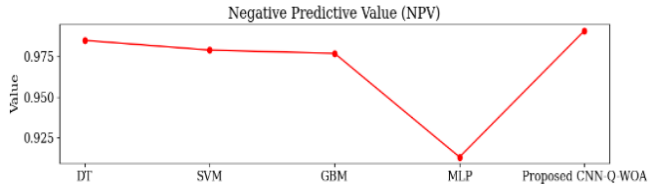
Table 4 and Figure 4, which presents the results of the RSA-TEO algorithm against traditional algorithms with an 90% learning rate, shows the comprehensive comparison of the algorithm performance times. The method in question demonstrates the enhanced performance across any significant measure. In the encryption time point of view, RSA-TEO is the fastest superseding the other methods, RNG, DHKE and traditional RSA, demonstrating considerable decrease in seconds needed for data encryption. The efficiency is not confined to encryption time alone as the RSA-TEO algorithm faster and more resourced oriented decryption process than the other algorithms.



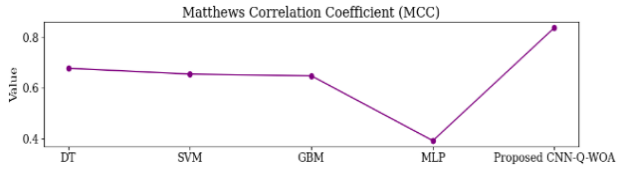
(a) False Negative Rate



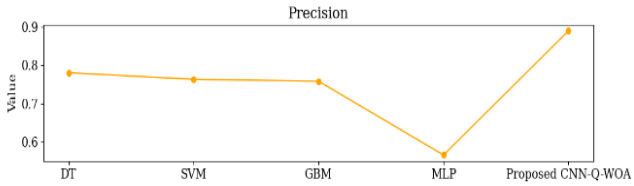
(b) False Positive Rate



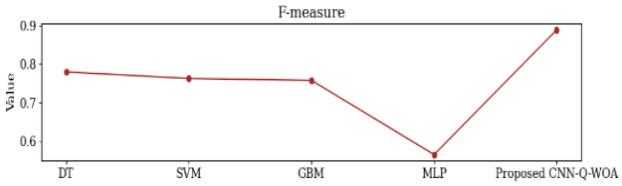
(c) Negative Predictive Value



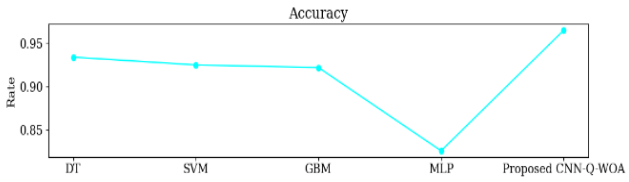
(d) Matthews Correlation Coefficient



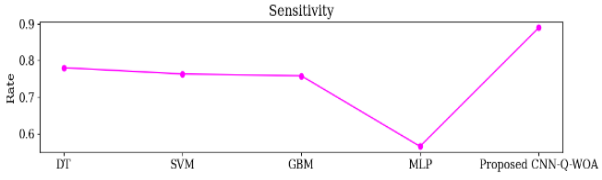
(e) Precision



(f) F-Measure

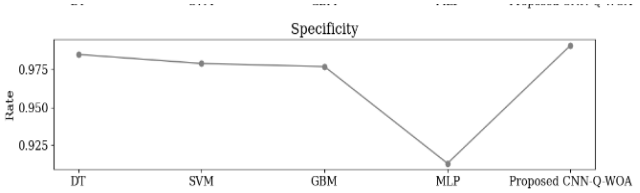


(g) Accuracy



(h) Sensitivity

RESEARCH ARTICLE



(i) Specificity

Figure 5 Comparison of Performance Metrics with 75% Learn Rate

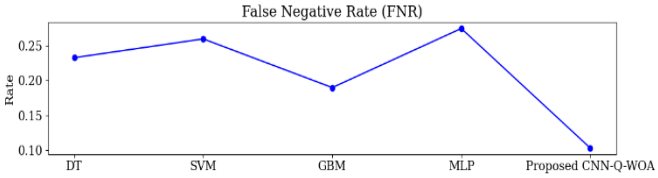
The RSA-TEO efficiency is also demonstrated through its low responsiveness time which sort of suggests an extremely responsive system. Generation time, a vital process of cryptographic algorithms, is highly improved in the proposed RSA-TEO algorithm. It is ahead of RNG, DHKE, and traditional RSA by demonstrating a simple and straightforward mechanism of key generation. RSA-TEO algorithm shows a remarkabal recovery capability, as measured by the restoration efficiency, which is the efficiency metric.

As seen in Table 5 and Figure 5, performance metrics, precision, specificity, accuracy, sensitivity, F-measure, MCC, NPV, FPR, and FNR, are visualized for different neural network models (Multilayer Perceptron (MLP), Decision Tree (DT), Support Vector Machine (SVM) and Gradient Boosting Machine (GBM)) and the proposed CNN-Q-WOA under 75% learning The suggested CNN-Q-WOA consistently outruns other models of neural networks on fundamental metrics for all evaluations. Regarding the accuracy, the proposed CNN-Q-WOA outperforms DT, MLP, SVM and GBM with 96.5% which is the highest among them These values illustrate a strong model that will be able to recognize the data points correctly. The suggested CNN-Q-WOA model performs significantly better than the other models in terms of precision, which is calculated by dividing the total number of true positive and false positive predictions by the number of true positive predictions. This higher precision suggests lower false positive rate, so we conclude that the model makes more accurate positive predictions.

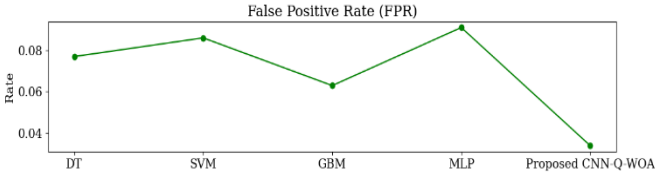
Another metric called sensitivity or recall measures the portion of true positives among the true positives. The designed CNN-Q-WOA shows a greater sensitivity (i.e. a higher capability of correctly identifying positive cases). It is, thus, more effective that DT, MLP, SVM and GBM. Differentiation, assessing the ratio of actual real negative cases to all true negative sample cases, is markedly better for the suggested CNN-Q-WOA.

The fact that it works well with negative instances means that it can effectively classify, leading to a more balanced classification. The CNN combined with Q-WOA has a significantly higher F-measure, a combined measure that related to precision and sensitivity. Such result can be regarded as a nuance between concentration and attentiveness that in a way culminates with the accuracy of the model. The MCC (Matthew's Correlation Coefficient), which incorporate many factors for classification, shows a significant higher value for proposed CNN-Q-WOA. This implies that there is a good connection between the estimate and reality, showing the model is generally a good one.

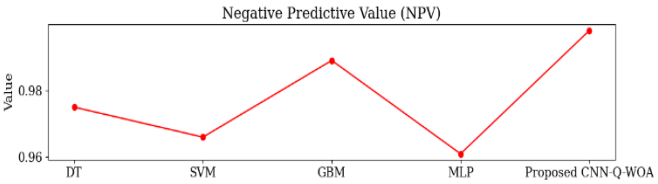
The Negative Predictive Value (NPV) demonstrates the percentage of true negatives among all negatives. This value for the mentioned CNN-Q-WOA model is remarkably bigger. This in fact means the low rate of false positives that the model produces which proves its ability to forecast the negative instances. The FPR and FNR values are substantially lower for the proposed CNN-Q-WOA model than other models. A lower FPR showed that there would be less false positive predictions, and a lower FNR showed that the model has less false negative predictions, that it helped with both positive and negative classification.



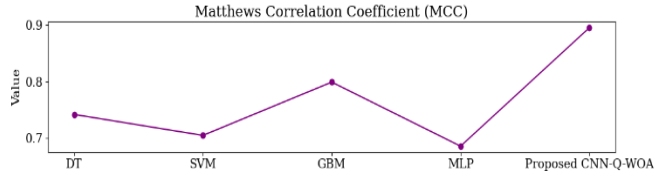
(a) False Negative Rate



(b) False Positive Rate

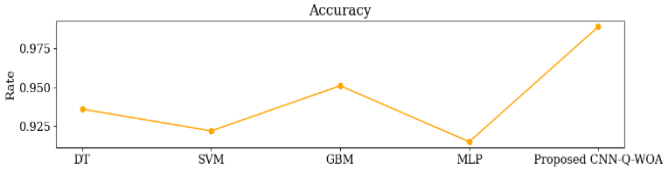


(c) Negative Predictive Value

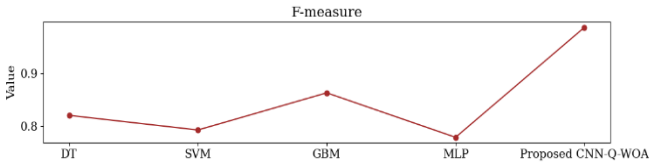


(d) Mattews Correlation Coefficient

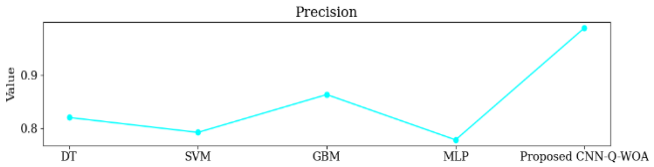
RESEARCH ARTICLE



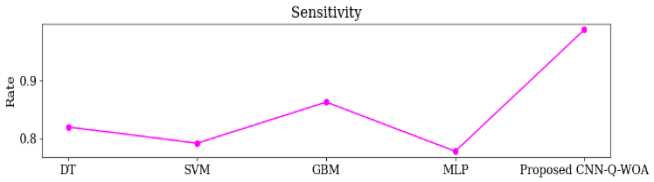
(e) Accuracy



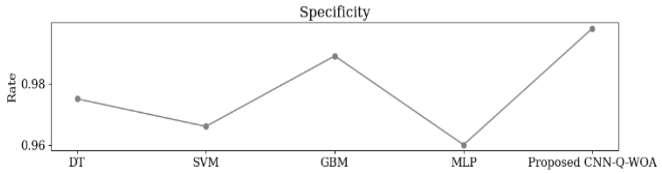
(f) F-Measure



(g) Precision



(h) Sensitivity



(i) Specificity

Figure 6 Comparison of Performance Metrics with 90% Learn Rate

Table 6 and Figure 6 portrays the performance evaluation of the major neural network models— DT, MLP, SVM, GBM —as well as the proposed CNN-Q-WOA under an 90% learning rate. Our proposed model CNN-Q-WOA brings superiority across several metrics compared to other models, confirming its capacity in detection of intrusions in the IoT networks. In terms of precision, the designed CNN-Q-WOA is able to reach the outstanding accuracy of 98.9%, which is much better than DT, MLP, SVM and GBM.

This incredible accuracy shows the strength and trustworthiness of the suggested model in identifying true instances in the data set. Accuracy, reflected in the true positive rate, of proposed CNN-Q-WOA model is evidently outstanding compared to other models. Such shows that the algorithm can do accurate positive predictions with a lower false alarms rate, thus improves the efficiency of intrusion detection.

Table 3 Comparison of Performance Time for 75% Learn Rate

Learn Rate 75%	RNG	DHKE	RSA	Proposed (RSA-TEO)
Restoration Efficiency	0.845	0.798	0.831	0.807
Sharing Record Time	13.442	14.036	13.180	13.012
Encryption Time	0.144	0.133	0.126	0.110
Key Generation Time	0.253	0.264	0.244	0.205
Response Time	215.312	224.423	210.886	209.007
Decryption Time	0.123	0.135	0.117	0.101

Table 4 Comparison of Performance Time for 90% Learn Rate

Learn Rate 90%	RNG	DHKE	RSA	Proposed (RSA-TEO)
Sharing Record Time	14.607	14.655	14.157	13.836
Response Time	233.724	234.493	226.518	223.101
Decryption Time	0.110	0.124	0.108	0.111
Restoration Efficiency	0.898	0.858	0.790	0.814
Encryption Time	0.118	0.127	0.125	0.101
Key Generation Time	0.228	0.251	0.234	0.102

RESEARCH ARTICLE

Table 5 Comparison of Performance Metrics with 75% Learn Rate

Learn Rate 75%	DT	SVM	GBM	MLP	Proposed CNN-Q-WOA
FNR	0.307	0.324	0.329	0.521	0.152
FPR	0.102	0.108	0.109	0.173	0.050
NPV	0.985	0.979	0.977	0.913	0.991
MCC	0.678	0.655	0.648	0.392	0.838
Precision	0.780	0.763	0.758	0.566	0.889
F_measure	0.780	0.763	0.758	0.566	0.889
Accuracy	0.934	0.925	0.922	0.826	0.965
Sensitivity	0.780	0.763	0.758	0.566	0.889
Specificity	0.985	0.979	0.977	0.913	0.991

Table 6 Comparison of Performance Metrics with 90% Learn Rate

Learn Rate 90%	DT	SVM	GBM	MLP	Proposed CNN-Q-WOA
FNR	0.233	0.260	0.190	0.275	0.103
FPR	0.077	0.086	0.063	0.091	0.034
NPV	0.975	0.966	0.989	0.961	0.998
MCC	0.742	0.705	0.799	0.686	0.895
Accuracy	0.936	0.922	0.951	0.915	0.989
F_measure	0.820	0.792	0.863	0.778	0.988
Precision	0.820	0.792	0.863	0.778	0.988
Specificity	0.975	0.966	0.989	0.96	0.998
Sensitivity	0.820	0.792	0.863	0.778	0.988

The sensitivity, or recall, of CNN-Q-WOA is constantly the best among the four competitors: DT, MLP, SVM and GBM. The higher sensitivity tells us about the ability of the model to accurately identify positive instances, thus demonstrating the effectiveness of the model in detecting the intrusion scenarios in the IoT networks. The specificity value is much higher in the suggested CNN-Q-WOA when compared to the traditional negative prediction measure. On the other hand, this mean that the model does well in differentiating between samples that are not intrusion and leaving a balanced classification. F-measure, an integrated evaluation of precision in addition to sensitivity is seeing a tremendous rise in the suggested CNN-Q-WOA. This speaks to how the model excellently balances these two measures, and it is highly effective in achieving both high precision and recall. The MCC, a measurement of the comprehensive performance of the classifier, is significantly high for the proposed CNN-Q-WOA. This pretty high concordance between estimated and real predictions implies the overall efficiency of the model. The Negative Predictive Value (NPV), that is a measure of accuracy of negative predictions, is majorly more exalted for the proposed CNN-Q-WOA.

The proposed CNN-Q-WOA significantly outperforms DT, MLP, SVM and GBM in a range of the metrics used as assessment tools under an 90% learning rate. These results, therefore, prove that the suggested model is more efficient as to the intrusions detection and it qualifies as a strong and complete tool for securing the IoT networks, all this due to the exceptional accuracy rate.

Table 7 Comparison of Detection Effects of Different Detection Algorithms

Methods	MTTD (in min)
DT	0.85
MLP	0.76
SVM	0.63
GBM	0.58
Proposed CNN-Q-WOA	0.41

Table 7 gives a thorough MTTD comparison for various intrusion detection algorithms, demonstrating their time-efficiencies in detection and timely addressing of events. The MTTD, being an important metric, tells about how fast detection is taking place and whether the algorithm is rapidly responsive or not. From the techniques tested, the CNN-Q-WOA presents the shortest time of detection and response by 0.41 min which shows its better performance in detection of security events quickly. Based on this, it can be inferred that the suggested CNN-Q-WOA model has more agile and responsive intrusion detection feature than traditional architecture of neural network like DT, MLP, SVM and GBM. The MTTD values of the above conventional models are higher than DT with 0.85 minutes, MLP with 0.76 minutes, SVM with 0.63 minutes, and GBM with 0.58 minutes. Hence, the proposed model which incorporates CNN-Q-WOA is the one that takes the centre stage in a situation where intrusion detection is to be done having its considerably lower mean time to detection.

5. DISCUSSION

The result shows that the proposed CNN-Q-WOA models exceed others in most metrics. The proposed CNN-Q-WOA model excels accuracy with 0.965, which is higher than the

RESEARCH ARTICLE

others, leading to the higher overall correct prediction rate. In addition to its accuracy (0.889) which is also the highest than that of other models, we can deduce that it produces fewer false positives. In the context of sensitivity measure, the Proposed-CNN-Q-WOA model (0.889) shows a higher rate of correctly predicting positive outcomes by causing fewer false negatives. Similarly, the best model succeeds in the aspect of its specificity (0.991) being higher than the other models indicating a small number of false positives.

The weight of being precise and correct at the same time is also higher for the Proposed CNN-Q-WOA model (0.889), because it shows better balance between these two measures. The Proposed CNN-Q-WOA model shows a significant advantage over the others with MCC of 0.838. This implication is due to better overall classification performance. Also, the NPV of the Proposed CNN-Q-WOA model (0.991) which has far less false negatives significance than the Baseline model can be remarked. Moreover, lower FPR and FNR are presented for Proposed CNN-Q-WOA (0.050 and 0.152 respectively) this implies that the model has comparatively lower rate of false positives and false negatives. Overall, therefore we see, this proposed model obtained outstanding performance compared to the other model showing the supremacy in terms of accuracy, precision, specificity, sensitivity, MCC, F-measure, NPV, FPR, and FNR.

Despite the comprehensive nature of this study, some limitations should be acknowledged to provide a nuanced understanding of the research context. This research is based on the NF-UQ-NIDS dataset, which the system is trained. The existence of some problems like it might not represent a variety of IoT situations and maybe some biases might influence the applicability of the proposed approach. Although some efforts have been taken to develop a testbed of IoT network environment with the purpose of presenting the real-life conditions, this simulation may not illustrate all the subtleties which are possible in the practical use.

6. CONCLUSION AND FUTURE SCOPE

6.1. Conclusion

This research provides a thorough examination of the creation and assessment of IoT framework for malware identification based on federated learning, with a focus on efficiency and robustness. The experimental setup involved the use of the NF-UQ-NIDS dataset to assess the proposed framework's performance under diverse network intrusion scenarios. The entire development cycle, executed in Python, prioritized the incorporation of strong cryptographic parameters. RSA-TEO algorithm came out as key player in generating of the optimum encryption keys resulting effective encryption process The use of the simulated IoT network environment, which imitates real-wold scenarios, created a platform for test run of the proposed framework in various network setups with attack scenarios. The experimentation comprised of training the CNN on the NF-UQ-NIDS dataset, which was further optimized with the help of Q-learning based whale optimization technique. The CNN serving as an IDS was placed within the IoT network which was constantly scanning and auditing network traffic to detect any potential intrusions. Simulation of various scenarios were perused to determine the defense systems competence while the proposed framework proved to be highly resilient to different security threats. In addition, the research went further and investigated the performance comparison of the suggested RSA-TEO algorithm with traditional key generation methods, for instance, Random Number Generation (RNG), Diffie-Hellman Key Exchange (DHKE), and the conventional RSA algorithm. The comparison provided the upper hand of RSA-TEO algorithm in terms of decryption time, encryption time, restoration efficiency, key generation time, response time, and sharing record time. The proposed CNN-Q-WOA model demonstrated an extraordinary ability to detect cyber intrusions outperformed other models on all critical metrics under both 75% and 90% learning rates.

6.2. Future Scope

The prospective directions of this study cover multifarious areas of inquiry and progress, pioneering the path towards the future improvements in the field of Blockchain and IoT security. The subsequent research can consider the modifications like attempts to increase its scalability or adaptability to the resource-constrained IoT devices which are often the challenge in the present time. The resilience against emerging cryptographic threats is also an important consideration.

REFERENCES

[1] Malhotra, P., Singh, Y., Anand, P., Bangotra, D.K., Singh, P.K. and Hong, W.C., 2021. Internet of things: Evolution, concerns and security challenges. Sensors, 21(5), p.1809.

[2] McGrath, McGrath RG. The end of competitive advantage: How to keep your strategy moving as fast as your business. Harvard Business Review Press; 2013 Jun 4.

[3] Ferrag, M.A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L. and Janicke, H., 2018. Blockchain technologies for the internet of things: Research issues and challenges. IEEE Internet of Things Journal, 6(2), pp.2188-2204.

[4] Alotaibi, B., 2019. Utilizing blockchain to overcome cyber security concerns in the internet of things: A review. IEEE Sensors Journal, 19(23), pp.10953-10971.

[5] Abdel-Basset, M., Abdel-Fatah, L. and Sangaiah, A.K., 2018. Metaheuristic algorithms: A comprehensive review. Computational intelligence for multimedia big data on the cloud with engineering applications, pp.185-231.

[6] Marini, F. and Walczak, B., 2015. Particle swarm optimization (PSO). A tutorial. Chemometrics and Intelligent Laboratory Systems, 149, pp.153-165.

[7] Mirjalili, Seyedali. "Evolutionary algorithms and neural networks." Studies in computational intelligence 780 (2019): 43-53.

RESEARCH ARTICLE

[8] Salehinejad, H., Sankar, S., Barfett, J., Colak, E. and Valaee, S., 2017. Recent advances in recurrent neural networks. arXiv preprint arXiv:1801.01078.
[9] Kattenborn, T., Leitloff, J., Schiefer, F. and Hinz, S., 2021. Review on Convolutional Neural Networks (CNN) in vegetation remote sensing. ISPRS journal of photogrammetry and remote sensing, 173, pp.24-49.
[10] Hassan, M.U., Rehmani, M.H. and Chen, J., 2019. Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. Future Generation Computer Systems, 97, pp.512-529.
[11] Gebremichael, T., Ledwaba, L.P., Eldefrawy, M.H., Hancke, G.P., Pereira, N., Gidlund, M. and Akerberg, J., 2020. Security and privacy in the industrial internet of things: Current standards and future challenges. IEEE Access, 8, pp.152351-152366.
[12] Sabillon, R., Cano, J.J. and Serra Ruiz, J., 2016. Cybercrime and cybercriminals: A comprehensive study. International Journal of Computer Networks and Communications Security, 2016, 4 (6).
[13] Peres, R., Schreier, M., Schweidel, D.A. and Sorescu, A., 2023. Blockchain meets marketing: Opportunities, threats, and avenues for future research. International Journal of Research in Marketing, 40(1), pp.1-11.
[14] Ma, B., Guo, W. and Zhang, J., 2020. A survey of online data-driven proactive 5G network optimisation using machine learning. IEEE access, 8, pp.35606-35637.
[15] Marwala, T., 2022. Closing the gap: The fourth industrial revolution in Africa. Pan Macmillan South Africa.
[16] Or-Meir, O., Nissim, N., Elovici, Y. and Rokach, L., 2019. Dynamic malware analysis in the modern era—A state of the art survey. ACM Computing Surveys (CSUR), 52(5), pp.1-48.
[17] Jing, Q., Vasilakos, A.V., Wan, J., Lu, J. and Qiu, D., 2014. Security of the Internet of Things: perspectives and challenges. Wireless Networks, 20, pp.2481-2501.
[18] Roman, R., Zhou, J. and Lopez, J., 2013. On the features and challenges of security and privacy in distributed internet of things. Computer networks, 57(10), pp.2266-2279.
[19] Al-Qarafi, A., Alrowais, F., S. Alotaibi, S., Nemri, N., Al-Wesabi, F.N., Al Duhayyim, M., Marzouk, R., Othman, M. and Al-Shabi, M., 2022. Optimal machine learning based privacy preserving blockchain assisted internet of things with smart cities environment. Applied Sciences, 12(12), p.5893.
[20] Seshadri, S.S., Rodriguez, D., Subedi, M., Choo, K.K.R., Ahmed, S., Chen, Q. and Lee, J., 2020. Iotcop: A blockchain-based monitoring framework for detection and isolation of malicious devices in internet-of-things systems. IEEE Internet of Things Journal, 8(5), pp.3346-3359.
[21] Alqaralleh, B.A., Vaiyapuri, T., Parvathy, V.S., Gupta, D., Khanna, A. and Shankar, K., 2021. Blockchain-assisted secure image transmission and diagnosis model on Internet of Medical Things Environment. Personal and ubiquitous computing, pp.1-11.
[22] Rathee, G., Ahmad, F., Sandhu, R., Kerrache, C.A. and Azad, M.A., 2021. On the design and implementation of a secure blockchain-based hybrid framework for Industrial Internet-of-Things. Information Processing & Management, 58(3), p.102526.
[23] Shen, M., Liu, H., Zhu, L., Xu, K., Yu, H., Du, X. and Guizani, M., 2020. Blockchain-assisted secure device authentication for cross-domain industrial IoT. IEEE Journal on Selected Areas in Communications, 38(5), pp.942-954.
[24] Unal, D., Hammoudeh, M., Khan, M.A., Abuarqoub, A., Epiphaniou, G. and Hamila, R., 2021. Integration of federated machine learning and blockchain for the provision of secure big data analytics for Internet of Things. Computers & Security, 109, p.102393.
[25] Issa, W., Moustafa, N., Turnbull, B., Sohrabi, N. and Tari, Z., 2023. Blockchain-based federated learning for securing internet of things: A comprehensive survey. ACM Computing Surveys, 55(9), pp.1-43.
[26] Razdan, S. and Sharma, S., 2022. Internet of medical things (IoMT): Overview, emerging technologies, and case studies. IETE technical review, 39(4), pp.775-788.
[27] S. Shen, L. Xie, Y. Zhang, G. Wu, H. Zhang, and S. Yu, "Joint differential game and double deep Q-networks for suppressing malware spread in Industrial Internet of Things," IEEE Transactions on Information Forensics and Security, vol. 18, pp. 5302–5315, Aug. 2023.
[28] G. Wu, L. Xie, H. Zhang, J. Wang, S. Shen, and S. Yu, "STSIR: An individual-group game-based model for disclosing virus spread in Social Internet of Things," Journal of Network and Computer Applications, vol. 214, May 2023, Art. no. 103608.
[29] Y. Shen, S. Shen, Q. Li, H. Zhou, Z. Wu, and Y. Qu, "Evolutionary privacy-preserving learning strategies for edge-based IoT data sharing schemes," Digital Communications and Networks, vol. 9, no. 4, pp. 906–919, Aug. 2023.
[30] S. Yu, R. Zhai, Y. Shen, G. Wu, H. Zhang, S. Yu, and S. Shen, "Deep Q-Network-based open-set intrusion detection solution for Industrial Internet of Things," IEEE Internet of Things Journal, 2023, http://dx.doi.org/10.1109/JIOT.2023.3333903.
[31] S. Shen, C. Cai, Z. Li, Y. Shen, G. Wu, and S. Yu, "Deep Q-Network-based heuristic intrusion detection against edge-based SIoT zero-day attacks," Applied Soft Computing, vol. 150, Jan. 2024, Art. no. 111080.
[32] S. Shen, X. Wu, P. Sun, H. Zhou, Z. Wu, and S. Yu, "Optimal privacy preservation strategies with signalling Q-learning for edge-computing-based IoT resource grant systems," Expert Systems with Applications, vol. 225, Sep. 2023, Art. no. 120192.
[33] Ficco, M., 2021. Malware analysis by combining multiple detectors and observation windows. IEEE Transactions on Computers, 71(6), pp.1276-1290.
[34] Kaveh, A., and Armin Dadras. "A novel meta-heuristic optimization algorithm: thermal exchange optimization." Advances in engineering software 110 (2017): 69-84.
[35] Zhang, Q., Zhang, M., Chen, T., Sun, Z., Ma, Y. and Yu, B., 2019. Recent advances in convolutional neural network acceleration. Neurocomputing, 323, pp.37-51.
[36] Alavizadeh, Hooman, Hootan Alavizadeh, and Julian Jang-Jaccard. "Deep Q-learning based reinforcement learning approach for network intrusion detection." Computers 11, no. 3 (2022): 41.
[37] Mirjalili, Seyedali, and Andrew Lewis. "The whale optimization algorithm." Advances in engineering software 95 (2016): 51-67.
[38] Jun, Benjamin, and Paul Kocher. "The Intel random number generator." Cryptography Research Inc. white paper 27 (1999): 1-8.
[39] Mäurer, Nils, Thomas Gräupl, Christoph Gentsch, and Corinna Schmitt. "Comparing different Diffie-Hellman key exchange flavors for LDACS." In 2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC), pp. 1-10. IEEE, 2020.
[40] Sihotang, Hengki Tamando, Syahril Efendi, Elvyawati M. Zamzami, and Herman Mawengkang. "Design and implementation of Rivest Shamir Adleman's (RSA) cryptography algorithm in text file data security." In Journal of Physics: Conference Series, vol. 1641, no. 1, p. 012042. IOP Publishing, 2020.
[41] NF-UQ-NIDS dataset, Available online at: https://staff.itee.uq.edu.au/marius/NIDS_datasets/

Author

Dr. Rami Baazeem is the head of the management information systems (MIS) department, college of business, University of Jeddah, KSA. Dr. Rami is a member of many national and international committees. Also, he is the head of the quality assurance unit, college of business, university of Jeddah. He has 15 years of experience in information systems and management. He had published many research papers related to e-commerce and data management. He attended many training courses in his specialization. He has awarded his Ph. D. from Kingston University, UK. Also, he has awarded his M. Sc. from Griffith University, Brisbane Australia. His research interests include data management, IT governance, e-commerce, and business intelligence.

RESEARCH ARTICLE

How to cite this article:

Rami Baazeem, "Multilayered Framework for Enhancing Data Confidentiality, Integrity, and Threat Detection through Blockchain, Advanced Cryptography, and Machine Learning", International Journal of Computer Networks and Applications (IJCNA), 11(5), PP: 556-576, 2024, DOI: 10.22247/ijcna/2024/36.