International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/14 Volume 12, Issue 2, March – April (2025)

RESEARCH ARTICLE

Device-to-Device (D2D) Wireless Communication Using Blockchain and Onion Routing

Kiran Bhavlal Jadhav
Department of Electronics Engineering, Kalinga University, Raipur, Chhattisgarh, India.
✉ jadhavkiran32@gmail.com

Manoj Kumar Nigam
Department of Electronics Engineering, Kalinga University, Raipur, Chhattisgarh, India.
manoj.nigam@kalingauniversity.ac.in

Sagar Bhilaji Shinde
Department of Computer Science and Engineering, Nutan Maharashtra Institute of Engineering and Technology, Pune, India.
sagar.shinde5736@gmail.com

Lalitkumar Wadhwa
Department of Computer Science and Engineering, Ajeenkya DY Patil University, Lohegaon, Pune, Maharashtra, India.
lalitkumarwadhwa@gmail.com

Pramod Patil
Department of Computer Science and Engineering, Dr. D. Y. Patil Institute of Institute of Technology, Pimpri, Pune, India.
pdpatiljune@gmail.com

Received: 12 January 2025 / Revised: 14 March 2025 / Accepted: 26 March 2025 / Published: 30 April 2025

Abstract – Device-to-device (D2D) communication has emerged as a critical technology in modern wireless networks, enabling efficient and cost-effective data exchange. However, its decentralized nature poses significant security and privacy challenges. This research proposes a novel methodology, Blockchain-based Onion Routing (BbOR) with Deep Convolutional Neural Networks (DCNN), to enhance the security, privacy, and robustness of D2D communication systems. Blockchain ensures data integrity and trustworthiness by maintaining an immutable, tamper-resistant ledger of encrypted tokens and messages. Onion routing adds a layer of privacy by anonymizing the communication path through multiple layers of encryption. The integration of Deep CNN for attack prediction enhances the system's ability to proactively detect and mitigate security threats, by analyzing token behavior and Blockchain transaction patterns. The proposed framework was validated using the Wireless Sensor Network Data Set (WSNDS), where data preprocessing, cryptographic token generation, secure routing, and attack detection mechanisms were systematically implemented. Results demonstrate the efficiency of the BbOR-Deep CNN system in providing robust security and privacy for D2D communication, making it suitable for applications in IoT, healthcare, and finance.

Index Terms – D2D Communication, Blockchain, Secure Routing, Privacy-Preserving Communication, Onion Routing, Deep Convolutional Neural Networks, Deep Learning-Based Attack Detection.

1. INTRODUCTION

Device-to-device (D2D) communication is a crucial component of IoT networks, addressing the increasing demands of mobile users while optimizing spectrum utilization [1]. Initially introduced in 4G networks, it has been further developed for 5G [2] to support applications such as smart factories, Industry 4.0, and real-time industrial automation [3]. By enabling direct communication between devices [4], D2D reduces network congestion, lowers power consumption, and improves data transmission efficiency [5].

Despite its benefits, D2D communication faces several challenges, including real-time activation [6], optimal

RESEARCH ARTICLE

spectrum allocation [7], and security vulnerabilities [8]. Researchers have explored various strategies to enhance performance, such as multi-hop cognitive wireless-powered communication for improving connectivity in Wireless Sensor Networks (WSNs) [9]. Graph-theoretic approaches have also been employed to enhance packet delivery by enabling direct communication between cluster heads [10]. Additionally, incentive mechanisms have been introduced in user-sharing-based caching systems to encourage participation and improve content distribution efficiency [11].

Security and privacy remain major concerns in D2D networks. Blockchain technology, known for its tamper-resistant and decentralized properties, ensures data integrity and prevents unauthorized modifications [12]. By providing immutable and transparent records, Blockchain enhances trust in caching and model training processes [13]. Given the complexity of 5G path selection, decentralized decision-making methods allow devices to optimize routing based on local information [14]. Meanwhile, Onion Routing strengthens privacy by encrypting messages in multiple layers [15] and routing them through intermediate nodes [16], thus preventing traffic analysis and preserving user anonymity [17].

However, existing methods such as Blockchain with Interplanetary File System (IPFS) introduce complexity [18], while traditional Fuzzy C-Means clustering may struggle in dynamic environments [19]. Mutual Authentication Schemes [20], although efficient, may not be suitable for networks with frequent device switching and multiple trust centers. Additionally, the security of Onion Routing heavily depends on user participation—reduced adoption can compromise anonymity. Therefore, enhancing its efficiency and integrating advanced security mechanisms are critical.

To address these challenges, this study proposes a Blockchain-based Onion Routing with Deep CNN (BbOR-DCNN) framework for secure D2D communication. Blockchain ensures transaction integrity, Onion Routing preserves privacy, and Deep CNN detects potential threats in real-time. This integrated approach enhances security, privacy, and resilience, making it well-suited for mobile networks, IoT systems, and peer-to-peer data exchanges.

1.1. Problem Statement

The integration of D2D communication with security mechanisms like blockchain and onion routing presents several research gaps. Current D2D protocols lack secure, privacy-preserving solutions, with traditional encryption methods being vulnerable. The application of blockchain in D2D communication, especially in mobile and IoT networks, is still underdeveloped, and existing onion routing protocols face challenges in minimizing delay and computational overhead. Additionally, proactive attack detection using machine learning, specifically Deep CNNs, has not been explored, and the integration of blockchain with CNNs for security threat detection remains novel. Scalability issues and the trade-off between real-time performance and security in decryption and authentication mechanisms further complicate D2D communication. The proposed research aims to address these gaps by combining blockchain, onion routing, and deep learning to create a secure, scalable, and privacy-preserving solution for D2D communication.

1.2. Motivation

With the rapid advancement of communication technologies, D2D communication has become a cornerstone of modern networks, particularly in the realms of mobile networks, IoT, and peer-to-peer data sharing. These technologies allow direct device communication, improving efficiency, speed, and cost-effectiveness, but also pose security and privacy risks, making data vulnerable to unauthorized access and attacks. As the number of connected devices grows, the risk of cyber threats like eavesdropping and data manipulation increases, with traditional security methods often falling short in decentralized, peer-to-peer networks. This study seeks to overcome challenges in secure communication by combining Blockchain and onion routing to enhance data integrity, privacy, and authentication. The proposed approach offers a reliable, scalable, and efficient solution for secure D2D communication, making it ideal for sensitive applications such as IoT, healthcare, and finance. Figure 1 illustrates the system model and problem statement.

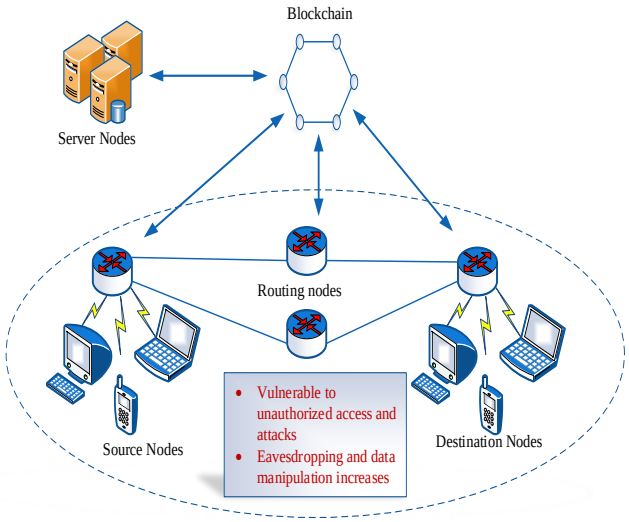

Figure 1 System Model and Problem Statement

A key contribution to the proposed method BbOR with Deep CNN:

- The input sensor data is collected by the transmitting device.

RESEARCH ARTICLE

- The input data is pre-processed to eliminate any irrelevant or unnecessary information.
- A unique cryptographic token is generated using pseudo-random methods, to serve as a one-time-use credential.
- The generated token is encrypted using a Diffie–Hellman algorithm, typically paired with the recipient's public key.
- The proposed BbOR-DCNN method is integrated where encrypted tokens and messages are stored within a Blockchain. The Blockchain ensures trust and immutability, providing a secure record of the transaction and preventing tampering.
- To further enhance security and privacy, onion routing is applied to the encrypted message. The data is encapsulated in multiple layers of encryption, with each intermediate node decrypting one layer at a time.
- An attack prediction mechanism with Deep CNN is incorporated into the BbOR method, utilizing Blockchain records and cryptographic token behavior to detect anomalies indicative of potential threats. This enables proactive threat detection and prevention.
- The destination device receives the encrypted message and token, validates its legitimacy by verifying the cryptographic hash, and ensures the token has not expired, been previously used, or mismatched with the Blockchain record.
- Once the token is validated, the encrypted message is decrypted using the shared secret or the recipient's private key.

Section 1 presents the topic, while Section 2 reviews previous studies and their associated challenges. Section 3 outlines the system model and the issues it faces. Section 4 details the proposed solution, followed by a discussion of the results in Section 5. Finally, Section 6 offers the conclusion.

2. RELATED WORK

To improve security and preserve reliable connections inside Machine-Type Communication (MTC), Jadav et al. [21] introduced the Garlic Routing Blockchain with Deep Learning. The Nadam optimizer, which is based on Long-Short-Term Memory (LSTM), first determines if incoming data requests are harmful or not. The Garlic Routing (GR) network receives non-malicious requests and assigns a unique ElGamal encrypted session tag to each participating computer. To protect the MTC data requests, Advanced Encryption Standard (AES) encryption is then used. To ensure scalability and secure management, the framework stores session tags on a blockchain based on the Inter-Planetary File System (IPFS). Furthermore, GRADE enhances network performance in MTC situations by utilizing the 6G network's capabilities. However, it is limited in the reliance on high network infrastructure for optimal performance.

Yaseen, et al. [22] showed an innovative approach of Onion Routing in Software Defined Networks to address the delay and interruption issues caused by the encryption, decryption, and cryptographic key exchange processes. The SDN layer facilitates intelligent and proactive management of Onion Routing network security information, enabling faster public key exchanges. The ML component optimizes the processing of security tasks, while the Blockchain ensures secure and tamper-proof management of cryptographic keys. This combination maintains continuous data flow for the clients, significantly improving network performance. However, challenges remain in the complexity of integrating SDN, ML, and BC technologies in the Tor network.

To enhance communication and energy efficiency in D2D-assisted decentralized learning, Liu, et al. [23] suggested The approach focuses on decentralized learning with joint optimization to adjust computational power, allocate wireless resources, select links, and adapt aggregate weights. By balancing learning latency with energy consumption, the goal is to minimize the total learning cost. This is achieved using a tabu search meta-heuristic for link selection, semi-definite programming for weight aggregation, and alternating optimization for computing power and wireless resource allocation. The disadvantage lies in the computational complexity of the optimization algorithms.

Yang et al. [24] proposed a selective Blockchain system with Byzantine fault tolerance to enhance D2D communication. The approach divides the Blockchain into off-blockchain and on-blockchain stages. In the first stage, it secures IoT devices transmitting sensitive data. The second stage focuses on improving privacy by assessing device security capacities and allowing devices to join a private Blockchain. The final stage optimizes consensus by evaluating node participation and detecting selfish participants. This method improves consensus reliability and performance for resource-limited environments. However, challenges include the complexity of off-blockchain management and scalability for large networks.

Luo, et al [25] used Deep learning approaches to optimize the age of information (AoI) and throughput. It addresses the limitation of traditional schemes that prioritize maximum throughput over information freshness. The proposed scheme utilizes a last-come-first-serve policy with packet replacement and leverages a neural network to learn optimal scheduling parameters without requiring explicit channel state information (CSI). This approach aims to strike a balance between maximizing throughput and minimizing AoI, resulting in improved overall system performance. However,

RESEARCH ARTICLE

it is limited in the trade-off between AoI and throughput metrics.

D2D communication facilitates direct data exchange for applications like public safety, V2V, and drones, requiring reliable connectivity across operators. Traditional roaming systems lack sufficient trust in D2D scenarios due to limited core network visibility of direct device links. To overcome this, Park et al. [26] introduced a Blockchain-inspired trust-based framework incorporating authentication, authorization, and class-aware dynamic resource pool selection. This approach enhances trust and resource efficiency, with analytical results demonstrating improved capacity through better decoding performance. While the framework offers benefits like improved reliability and resource management, its complexity and implementation costs remain challenges.

Miao et al. [27] address challenges in wireless IoT, such as spectrum reuse, network efficiency, and security in 5G, by proposing a D2D group communication protocol. The protocol employs the Chinese Remainder Theorem, secret sharing, and Chebyshev Polynomials to enable secure and efficient group authentication. Validated through BAN logic and security analysis, it demonstrates superior security and performance compared to existing methods. While the approach enhances efficiency, its design and implementation add complexity to the system.

Kiran et.al [28] explored the potential of combining Onion Routing and Blockchain technology to enhance wireless data transfer security, particularly in industries like healthcare, finance, and government. However, it acknowledges performance trade-offs like higher latency and energy consumption.

J. Kiran et.al [29] presented a hybrid architecture combining Blockchain and onion routing for enhanced privacy and security. Results show that it is particularly suitable for smart cities, healthcare, and finance, reduces attack success rates and resource usage. Future optimizations aim to optimize the framework for limited resource contexts and improve user data security.

The details of existing work with their advantage and disadvantages are mentioned in Table 1.

Table 1 Challenges of Existing Works

Sr. No.	Author	Method	Merits	Demerits
1.	Jadav et al. [21]	Garlic Routing Blockchain with Deep Learning	It ensures scalability and secure management	It is limited in the reliance on high network infrastructure for optimal performance.
2.	Yaseen, et al. [22]	Onion Routing in Software Defined Network	It significantly improves network performance.	Challenges remain in the complexity of integrating SDN, ML, and BC technologies in the Tor network.
3.	Liu, et al. [23]	Decentralized Learning with Joint Optimization Algorithm	It reduces the overall learning cost	High computational complexity of the optimization algorithms
4.	Yang, et al [24]	Selective blockchain and byzantine fault tolerance method	It improves the reliability of the consensus mechanism and overall system performance	Challenges include the complexity of off-blockchain management and scalability for large networks.
5.	Luo, et al [25]	Deep learning approaches	It improves overall system performance.	It is limited in the trade-off between AoI and throughput metrics.
6.	Park et al. [26]	Blockchain-inspired trust-based framework	It improves reliability and resource management	It is limited by complexity and implementation costs
7.	Miao et al. [27]	D2D group communication protocol	the approach enhances efficiency	Its design and implementation add complexity to the system.

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/14 Volume 12, Issue 2, March – April (2025)

RESEARCH ARTICLE

3. PROPOSED MODELLING

A novel method of Blockchain-based Onion routing with Deep CNN (BbOR-DCNN) in D2D communication is developed by enhancing the security and privacy of the data. Blockchain offers a secure, transparent platform for recording device transactions, ensuring data integrity, and detecting any alterations. Its decentralized nature eliminates single points of failure, enhancing system resilience against attacks. Onion routing ensures data confidentiality and data privacy by encrypting the message multiple times and routing it through several nodes, each removing one layer of encryption, preventing eavesdropping, and preserving sender and recipient anonymity. By combining these technologies, the proposed methodology achieves a high level of security and privacy for D2D communication, making it suitable for a wide range of applications, including mobile communications, IoT networks, and peer-to-peer data exchanges.

Figure 2 illustrates the architecture of the proposed BbOR-DCNN model, which enhances secure D2D communication by integrating Blockchain, Onion Routing, and Deep CNN for attack prediction. Initially, the transmitting device generates input data, applies preprocessing for quality enhancement, and creates a cryptographic token using pseudo-random methods. This token is encrypted with the Diffie-Hellman algorithm and paired with the recipient's public key for secure transmission. The encrypted token and message are stored in a Blockchain to ensure integrity. Onion routing adds multiple encryption layers, which intermediate nodes decrypt sequentially to maintain privacy. Deep CNN analyzes Blockchain records to detect threats. At the destination, the token is validated, and upon success, the message is decrypted using the shared secret or recipient's private key.

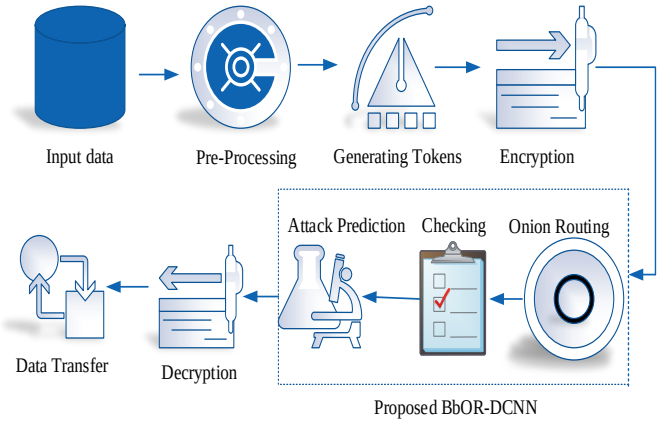

Figure 2 Architecture of Proposed BbOR-DCNN

3.1. Data Collection

The "WSNDS" (Wireless Sensor Network Data Set) on Kaggle consists of data collected from a wireless sensor network deployed to monitor environmental conditions. It includes sensor readings such as temperature, humidity, and other environmental parameters gathered from various sensor nodes over time. The dataset is designed to facilitate research in areas like sensor network data analysis, anomaly detection, and environmental monitoring.

It provides a comprehensive collection of time-series data, making it valuable for machine-learning models aimed at predictive maintenance, sensor calibration, and energy-efficient network management in wireless sensor networks.

https://www.kaggle.com/datasets/bassamkasasbeh1/wsnds

3.2. Data Preprocessing

In this study, the preprocessing [30] step involves standardizing the sensor dataset to ensure consistency and comparability across variables. Standardization adjusts the data to have a mean of 0 and a standard deviation of 1, enhancing the performance of subsequent analysis and modeling. The standardization Y_{St} formula is given in equation (1):

$$Y_{St} = \frac{Y - M(Y)}{D(Y)} \quad (1)$$

Here, Y represents the individual sensor data value being standardized. The mean $M(Y)$ refers to the average value of the sensor data distribution, while the standard deviation $D(Y)$ measures the dispersion of the data. This transformation ensures that all sensor data variables are on a similar scale, reducing bias and improving the robustness of the proposed methodology.

3.3. Cryptographic Token Generation Using CSPRNG

The proposed method employs Cryptographically Secure pseudorandom number Generators (CSPRNGs) [31] to generate highly secure and unpredictable tokens. An 8-byte nonce is generated using CSPRNG: "MHkxbV9Q", which is then concatenated with the cryptographic token: "WNE7Bc4bsi6r02x9ECQTBmDph77JHXVk", forming the final token:

"MHkxbV9QWNE7Bc4bsi6r02x9ECQTBmDph77JHXVk"

This combined token is securely stored in cryptographic_token_with_nonce.txt for encryption, authentication, or validation, ensuring robust security in D2D communication.

3.4. Token Encryption Using

In this work, the Diffie–Hellman (DH) algorithm [32] is utilized to securely encrypt a cryptographic token by generating a common secret key shared between the sender

RESEARCH ARTICLE

and recipient. A large prime G and a primitive root modulo G, denoted as R are chosen as public parameters.

The sender selects a private key $s \in [1, G-1]$ and computes their public key $s_k \in [1, G-1]$ $s_k = R^s \pmod G$. For instance, the sender's public key is $s_k = 16$. Similarly, the recipient chooses a private key $r \in [1, G-1]$ and computes their public key $r_k = R^r \pmod G$. For instance, the recipient's public key is $r_k = 3$.

The sender and recipient exchange public keys and each independently calculates the shared secret key by raising the received public key to the power of their private key modulo G. The sender computes the shared secret $S_{sr} = S_r^s \pmod G = R^{sr} \pmod G$. The recipient independently computes $S_{rs} = S_s^r \pmod G = R^{rs} \pmod G = S_{sr}$. Both computations yield the same shared secret $S_{Shared} = R^{sr} \pmod G$.

This shared secret is then used as a symmetric key to encrypt the token, producing the encrypted token. Each byte of the token is transformed using the shared key, resulting in the encrypted token E^{TK} s "131,149,158,163,153,164,153,166,149,125,149,163,163,145, 151,149".

The DH process can be interpreted as a dynamical system where key generation and shared secret computation are modeled as iterative processes. For key generation, the dynamical system is defined in equation (2)

$$w_{n+1} = R \cdot w_n \bmod G \;\; with \;\; w_0 = 1 \quad (2)$$

This progression leads to the public keys s_k and r_k, which are endpoints of the respective trajectories for the sender and recipient. For shared secret computation, another system evolves as $z_{n+1} = r_k \cdot z_n \bmod G$ for the sender and $z_{n+1} = s_k \cdot z_n \bmod G$ for the receiver, both starting with $z_0 = 1$. This ensures that the computed shared secrets $S_{rs} = z_s$ (sender) and $S_{sr} = z_r$ (recipient) are equal, forming the common secret key.

By securely deriving the shared secret S_{Shared}, the encrypted token can only be decrypted by the recipient who possesses the private key r, ensuring the confidentiality of the token.

3.5. Blockchain Based Onion Routing

This work employs Blockchain-based onion routing to ensure secure and anonymous D2D communication. After encrypting the verification token using Diffie-Hellman (DH) key exchange, Blockchain securely distributes the encrypted token and messages among participating devices. Each transaction generates a block containing the encrypted token, message, device ID, and timestamp, which is hashed and appended to the Blockchain, ensuring integrity, transparency, and tamper resistance.

For routing, layered encryption is applied, where each layer corresponds to an intermediate device's public key. As the message traverses the network, each device decrypts one layer using its private key, extracts the verification token, and appends it to the shared secret key for further decryption. This preserves sender and recipient anonymity while protecting communication from malicious actors.

The integration of Blockchain and onion routing [33] enhances the security, privacy, and trustworthiness of the D2D communication network.

The encrypted token E^{TK}, along with the message and device details, is securely stored in the Blockchain B_C. Blockchain ensures transparency, trust, and immutability. Each block in the Blockchain contains: an encrypted verification token E^{TK}, the encrypted message E_M, the device ID, and a timestamp T_S. To create a block, a hash is computed for the current block using a combination of the hash of the previous block h_{V-1}, the encrypted token for the current device E_V^{TK}, and a randomly generated nonce N_V for validation. The hash h_V value for the V^{th} block is calculated using equation (3):

$$h_V = h_{V-1} \oplus E_V^{TK} \oplus N_V \quad (3)$$

where, the operator $\oplus$ represents a bitwise XOR operation, which ensures that the resulting hash is unique and depends on all the input elements. This process links each block cryptographically to its predecessor, creating a secure and immutable chain of records. Once the block hash is validated and consensus is achieved among the participating nodes, the block is appended to the Blockchain. This ensures integrity, transparency, and protection against tampering.

3.5.1. Onion Routing for Anonymized Communication

Onion routing enables secure message delivery by applying layered encryption, where each layer corresponds to an intermediate device's public key P_n of the n device. The

RESEARCH ARTICLE

sender encrypts the message M in multiple layers, ensuring secure transmission across the communication path. The fully encrypted message E_M is computed using equation (4):

$$E_M = E_{P_n}\left(E_{P_{n-1}}\left(E_{P_1}(E)\right)\right) \quad (4)$$

Here, E_{P_n} denotes encryption using the public key P_n. The fully encrypted message E_M and the Blockchain transaction ID β, which securely stores associated metadata and tokens, are transmitted to the first device. Each device decrypts its layer using its private key P_{De}^K, revealing the next layer, and ensuring secure, stepwise processing of the message.

The message is routed through multiple intermediate devices. At each intermediate device I_{De}. One layer of encryption is removed using the device's private key P_{De}^K. The device uses its private key P_{De}^K to decrypt the verification token E^{TK} and is defined using equation (5)

$$E_{decrypt}^{TK} = I_{P_{De}^K}\left(E^{TK}\right) \quad (5)$$

Then the decrypted verification token $E_{decrypt}^{TK}$ is appended to the device's shared secret S_{Shared}^{De} to decrypt the corresponding onion layer, as shown in equation (6):

$$\hat{S}_{Shared}^{De} = S_{Shared}^{De} + E_{decrypt}^{TK} \quad (6)$$

This step reveals the next layer of the encrypted message while keeping the remaining layers secure. The device then passes the partially decrypted message to the next intermediate device along the path. Throughout the process, Blockchain ensures secure storage of the encrypted token E^{TK}, maintaining data integrity and granting decryption access only to authorized devices.

3.6. Attack Prediction

A Deep CNN (DCNN) predicts potential attacks by analyzing features from Blockchain records and cryptographic token behavior. It processes input through convolutional, pooling, and fully connected layers [34], extracting hierarchical features to classify traffic as normal or malicious using a softmax function.

Let A represent input features derived from Blockchain data, including token metadata, hash values, timestamps, and detected anomalies. The DCNN extracts hierarchical features using convolutional filters, with the convolutional layer L_{C_t} output represented by equation (7).

$$L_{C_t} = \mathrm{Re}\,LU\left(C\left(A, F_t\right)\right) \quad (7)$$

Where $C\left(A, F_t\right)$ represents convolution operation with filter F_t, $\mathrm{Re}\,LU(z)$ is the rectified linear unit activation function. The output of each pooling layer reduces the spatial dimensions, the output of the t^{th} pooling layer is defined using equation (8):

$$L_{P_t} = Pool_t\left(L_{C_t}\right) \quad (8)$$

where $Pool_t$ represents the pooling operation. The final pooling layer's output is flattened into a one-dimensional vector and passed through fully connected layers ($f_c^1, f_c^2, \ldots . f_c^n$). ω_n is taken as the weight for the fully connected layers. The softmax activation function is applied O^n , yielding probabilities for each class as shown in equation (9):

$$B = Soft\max\left(f_c^n\left(O^n\right)\right) \quad (9)$$

The output O^n from the final fully connected layer is derived by applying the weights ω_n to the preceding layer's output. The softmax function then transforms this output into a probability distribution across the two classes, distinguishing between normal and attack categories. The training process minimizes cross-entropy loss to improve prediction accuracy. If the probability of an attack exceeds a predefined threshold, the message is flagged for security review. Otherwise, it proceeds to the decryption stage, ensuring secure and proactive threat detection before the final message is decrypted at the destination device.

3.7. Decryption at the Destination Device

After the attack prediction stage, the message decryption process occurs at the destination device. Once the Deep CNN has analyzed the Blockchain records and cryptographic token behavior to predict and detect potential attacks, the destination device proceeds with decrypting the message. If no threats are identified and the token and message are verified, the device decrypts the message using the shared secret or its private key. This step guarantees that only the intended recipient, possessing the correct key, can access the original content. The combination of Blockchain-based token validation, attack prediction through Deep CNN, and final decryption ensures

RESEARCH ARTICLE

secure, trustworthy, and tamper-resistant communication between devices in the D2D network. A pseudocode of the Proposed BbOR-DCNN method in D2D Wireless communication is given in Algorithm 1. Flow chart of the proposed method is given in Figure 3.

Start

{

Data Collection

{

// gathering wireless sensor network data

}

Data preprocessing

{

$Int\ \ Y_{St}, Y, M, D$

// initialize the preprocessing parameters $Y_{St} = \frac{Y - M(Y)}{D(Y)}$

//using equation (1)

//Standardized the sensor data

}

Cryptographic Token Generation

{

// Tokens are generated using CSPRNG for high security

// Generate an 8-byte nonce (e.g., MHkxbV9Q)

// Generate a secure cryptographic token using CSPRNG (WNE7Bc4bsi6r02x9ECQTBmDph77JHXVk)

// Concatenate nonce and token to form a unique token (MHkxbV9QWNE7Bc4bsi6r02x9ECQTBmDph77JHXVk)

}

Token Encryption using Diffie-Hellman

{

$Int\ \ s, r, s_k, r_k, S_{Shared}$

// initialize the encryption parameters

// sender chooses private key $s \in [1, G-1]$ and computes public key $s_k \in [1, G-1]$

// receiver chooses private key $r \in [1, G-1]$ and computes public key $r_k = R^r \pmod G$

//The sender and recipient exchange public keys and compute the shared secret

$S_{Shared} = R^{sr} \pmod G$

// This shared secret is then used to encrypt the token E^{TK} for secure transmission

}

Proposed BbOR-DCNN

{

Blockchain-Based Onion Routing

{

$Int\ \ h_V, E_M, E^{TK}, I_{P_{De}^K}, \hat{S}_{Shared}^{De}$

// Initialize the parameters

//Combining blockchain and onion routing achieves secure and anonymous communication

//Each transaction creates a new block with an encrypted verification token E^{TK}, the encrypted message E_M, the device ID, and a timestamp T_S

$h_V = h_{V-1} \oplus E_V^{TK} \oplus N_V$ // using equation (3)

// hash h_V value for the block is calculated

// sender applies multiple layers of encryption to the message using onion routing

// At each intermediate device I_{De} one layer of encryption is removed using the device's private key

$E_M = E_{P_n}\left(E_{P_{n-1}}\left(E_{P_1}(E)\right)\right)$ // using equation (4)

// message encrypted

$E_{decrypt}^{TK} = I_{P_{De}^K}\left(E^{TK}\right)$ // using equation (5)

// the decrypt verification token

$\hat{S}_{Shared}^{De} = S_{Shared}^{De} + E_{decrypt}^{TK}$ // using equation (6)

// decrypted verification token is combined with the device's shared secret S_{Shared}^{De} to decrypt the corresponding onion layer

}

RESEARCH ARTICLE

Attack Prediction using DCNN

{

$$Int \;\; h_V, E_M, E^{TK}, I_{P_{De}^K}, \hat{S}_{Shared}^{De}$$

// Initialize the prediction parameters

$$L_{C_t} = \mathrm{Re}\,LU\left(C\left(A, F_t\right)\right)$$ // using equation (7)

// hierarchical features are extracted using filters in the convolution layer

$$L_{P_t} = Pool_t\left(L_{C_t}\right)$$ // using equation (8)

//The spatial dimensions reduced in each pooling layer

//The final pooling layer's output is flattened into a one-dimensional vector and passed through fully connected layers

$$B = Soft\max\left(f_c^n\left(O^n\right)\right)$$ // using equation (9)

// the softmax activation function is applied to O^n, yielding probabilities for each class

}

Decryption at the destination device

{

If

no threats are detected the received message decrypted

Else

stop

}

}

End

}

Algorithm 1 Pseudocode of the Proposed BbOR-DCNN Method in D2D Wireless Communication

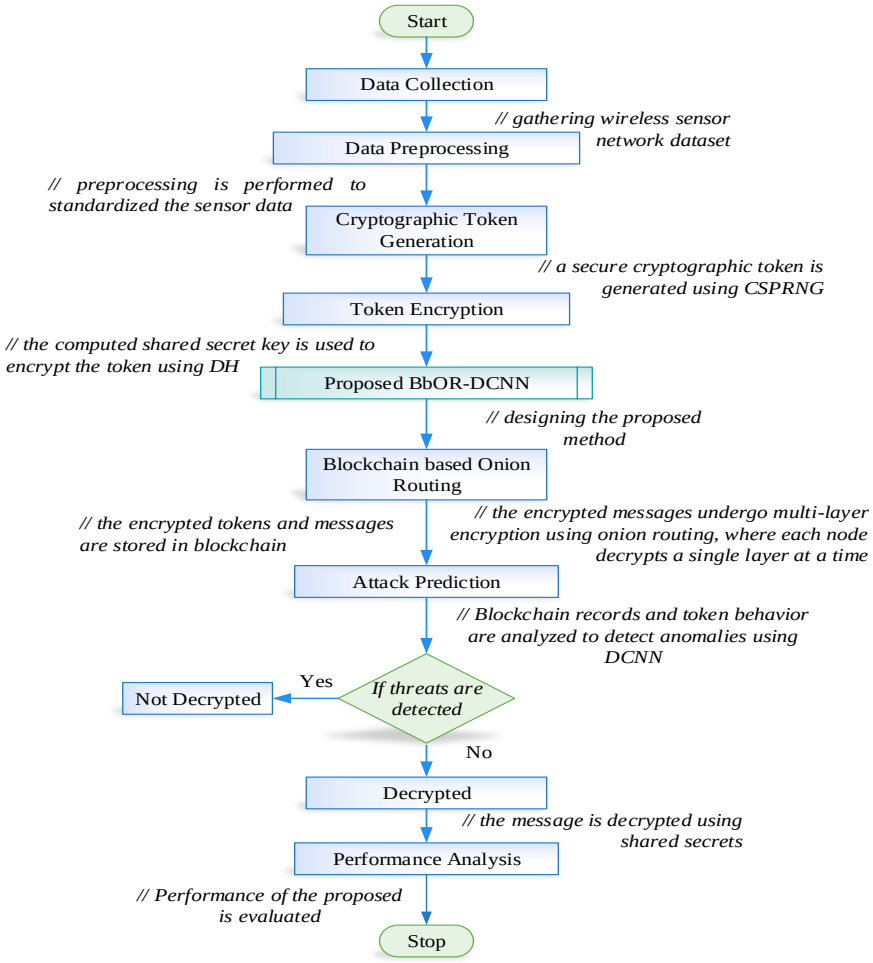

Figure 3 Flowchart of the Proposed BbOR-DCNN Approach

RESEARCH ARTICLE

4. RESULTS AND DISCUSSIONS

The proposed method BbOR-DCNN is implemented in MATLAB to simulate and analyze secure communication in D2D networks, focusing on the integration of Blockchain and onion routing for enhanced privacy and data integrity. The performance of the proposed BbOR-Deep CNN is evaluated using accuracy, packet delivery ratio, average energy consumption, data delay, computational complexity, prediction time, encryption time, and decryption time.

Table 2 provides details of the experimental setup used for the evaluation. MATLAB is chosen for simulation in this study due to its robust computational capabilities, specialized toolboxes, and ease of prototyping complex algorithms for secure D2D communication using blockchain and onion routing (BbOR).

Unlike NS-3, which is ideal for protocol-level simulations, it lacks built-in support for cryptographic security modeling, blockchain validation mechanisms, and deep learning-based anomaly detection, or Python-based frameworks such as TensorFlow and PyTorch, which primarily focus on deep learning, but do not provide the same level of integrated network security modeling, cryptographic token handling, and real-time data encryption as MATLAB.

MATLAB provides a well-integrated environment for both cryptographic security modeling and deep learning-based attack detection. The BbOR-DCNN framework requires extensive cryptographic processing, blockchain-based token validation, and onion routing implementation, all of which are efficiently supported by MATLAB's built-in functions. Additionally, MATLAB's superior data visualization and matrix-based computation efficiency allow for a detailed analysis of key security performance metrics, including packet delivery ratio, encryption time, computational complexity, and adversarial attack resilience.

These advantages make MATLAB the optimal choice for designing, testing, and validating the proposed BbOR-DCNN framework, ensuring its robustness and efficiency in securing D2D communication against evolving cyber threats.

Table 2 Experimental Setup for the Proposed Method

Parameter Description	
Processor	Intel(R) Core(TM) i5-4300M CPU @ 2.60GHz 2.60 GHz
Installed RAM	8.00 GB
Version	22H2
Edition Windows	10 Pro
Platform	MATLAB R2023a

4.1. Experimental Analysis

The test accuracy graph in Figure 4 of the proposed method shows a rapid improvement in performance within the initial epochs, achieving nearly 100% accuracy by the second epoch. The smoothed accuracy remains consistently high throughout the training process, with minimal fluctuation, indicating robust learning and convergence of the model. The loss graph also reflects this stability, with a sharp decrease in the initial epochs and a gradual decline to near zero as the epochs progress, demonstrating efficient minimization of the error function. The model's training process is efficient, completing in just 10 epochs with a constant learning rate of 0.001, showcasing its reliability and effectiveness.

4.2. Evaluation of the Proposed System's Performance

The proposed method of BbOR-DCNN in D2D communication is developed by enhancing the security and privacy of the data. The performance of the proposed method is evaluated using metrics such as accuracy, packet delivery ratio, average energy consumption, data delay, computational complexity, prediction time, encryption time, and decryption time.

4.2.1. Accuracy

In the proposed BbOR-DCNN work, accuracy R_A represents the model's ability to correctly predict outcomes based on input data. This is crucial for assessing how well the Deep CNN learns and generalizes patterns in data after optimization by BbOR. The accuracy is expressed using the equation (10). Higher accuracy indicates better reliability and correctness of the proposed approach.

$$R_A = \frac{T_P+T_N}{T_P+T_N+F_P+F_N} \quad (10)$$

Where, true positive (T_P) and true negative (T_N) to the ratios of all true positive (T_P), true negative (T_N), false positive (F_P), and false negative (F_N) values. The proposed method achieved a higher accuracy as shown in figure 5.

4.2.2. Packet Delivery Ratio

In the proposed BbOR routing mechanism, PDR assesses the routing efficiency by determining the ratio of successfully delivered data packets to the total transmitted packets. Higher PDR indicates robust routing decisions made by BbOR. A high PDR reflects the effectiveness of the BbOR in minimizing packet loss and ensuring reliable data transmission. The proposed method achieved a better PDR as shown in the figure 6.

4.2.3. Average Energy Consumption

This metric evaluates the energy efficiency of BbOR in managing network resources and minimizing the energy drained during data transmission and computation. Lower

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/14 Volume 12, Issue 2, March – April (2025)

RESEARCH ARTICLE

average energy consumption indicates better energy optimization by the BbOR mechanism. Figure 7 shows the average energy consumption of the proposed approach.

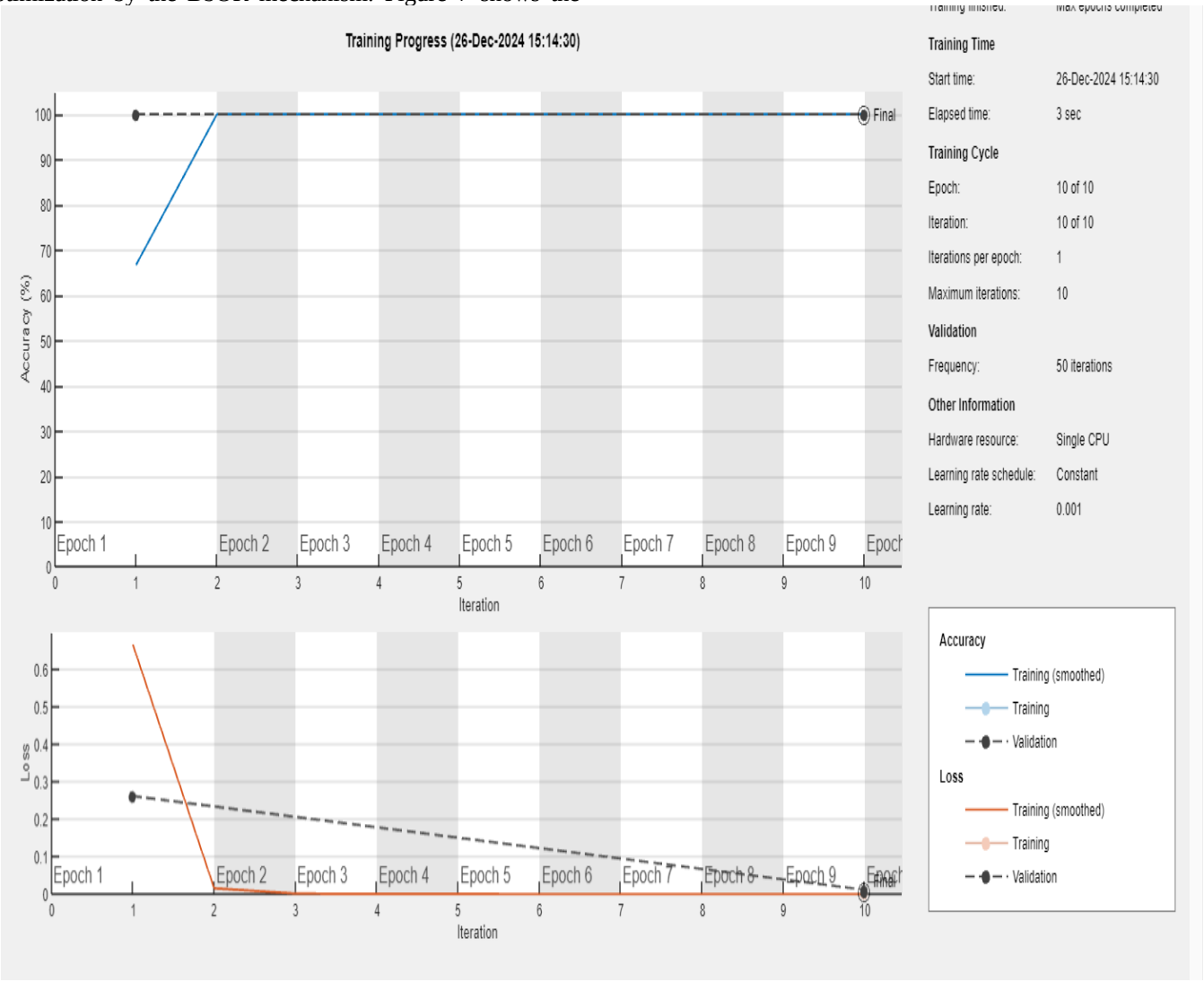

Figure 4 Test Accuracy of the Proposed Approach

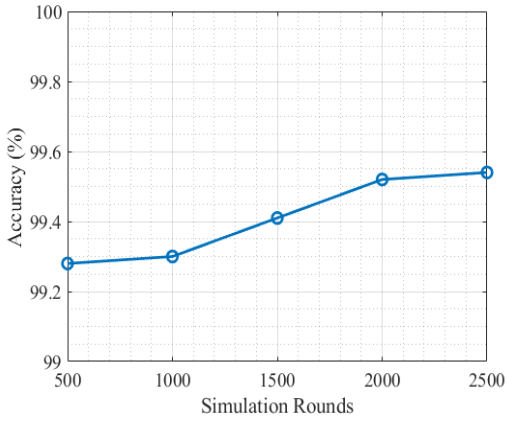

Figure 5 Accuracy of the Proposed BbOR-DCNN

RESEARCH ARTICLE

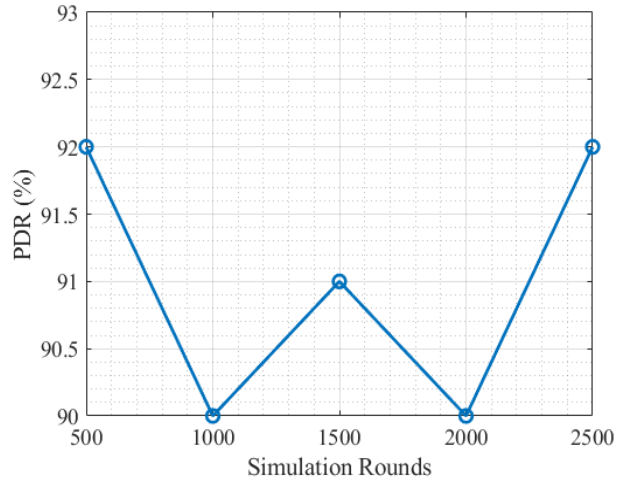

Figure 6 PDR of the Proposed BbOR-DCNN

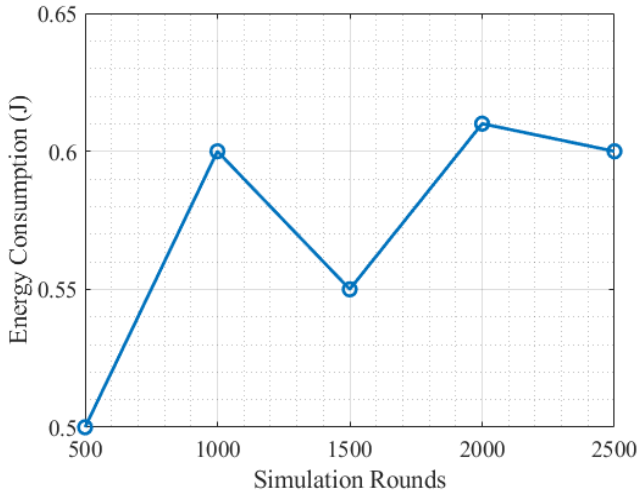

Figure 7 Energy Consumption of the Proposed BbOR-DCNN

4.2.4. Data Delay

Data delay measures the time taken for packets to reach the destination, reflecting the routing efficiency of BbOR and the prediction speed of Deep CNN. Minimizing delay is critical for real-time applications. The delay is impacted by routing optimization BbOR and the computational efficiency of the Deep CNN. Figure 8 illustrate the performance of the data delay achieved by the proposed approach.

4.2.5. Computational Complexity

The computational complexity evaluates the BbOR-DCNN system in terms of time and space. For BbOR-Deep CNN, the overall complexity considers the optimization cost of BbOR and the inference cost of DCNN. The proposed method achieved a better computational complexity as shown in the figure 9.

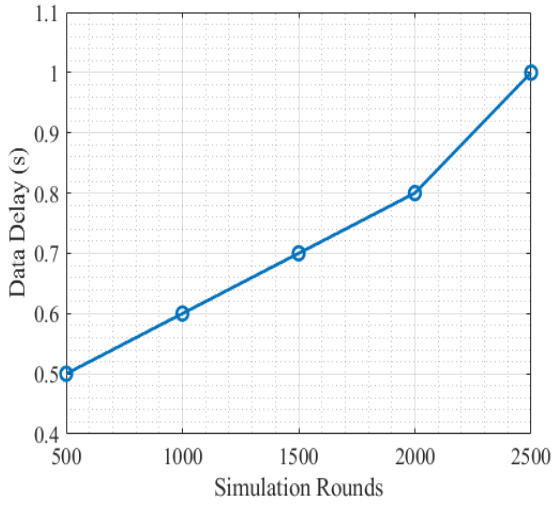

Figure 8 Data Delay of the Proposed BbOR-DCNN

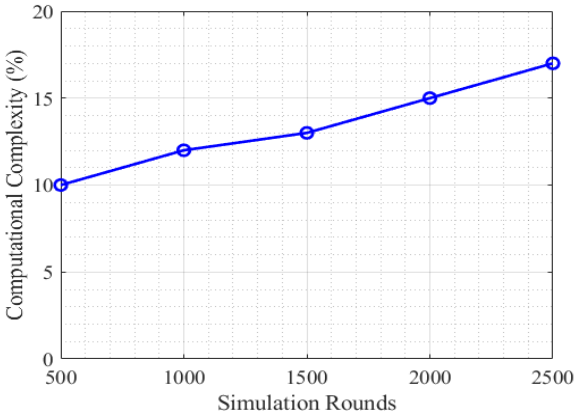

Figure 9 Computational Complexity of the Proposed BbOR-DCNN

4.2.6. Prediction Time

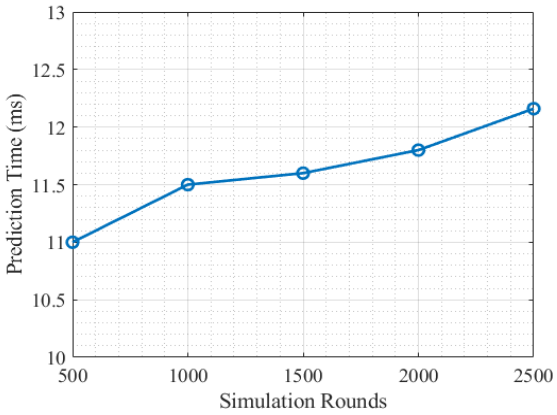

Figure 10 Prediction Time of the Proposed BbOR-DCNN

RESEARCH ARTICLE

Prediction time is the time required for the Deep CNN to infer a result from given input data. It reflects the efficiency of the BbOR-Deep CNN in providing quick and accurate predictions. Lower prediction times signify a faster and more efficient Deep CNN model. The proposed method achieved a lower prediction time as shown in the figure 10.

4.2.7. Encryption time

In the proposed framework, encryption time refers to the time taken to secure data for transmission during the routing process managed by BbOR. Efficient encryption ensures data security without significant overhead. The proposed method achieved a lower encryption time as shown in the figure 11.

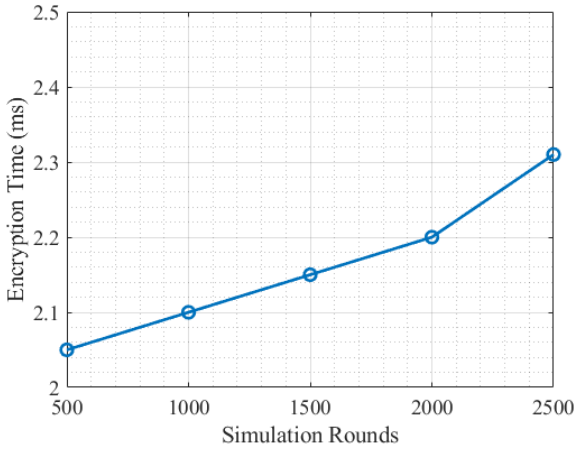

Figure 11 Encryption Time of the Proposed BbOR-DCNN

4.2.8. Decryption time

Decryption time measures the time needed to decrypt the data at the destination. This is important for ensuring seamless data usage in secured communication scenarios. It reflects the security mechanisms integrated into BbOR for protecting data during transmission. The proposed method achieved a lower decryption time as shown in the figure 12.

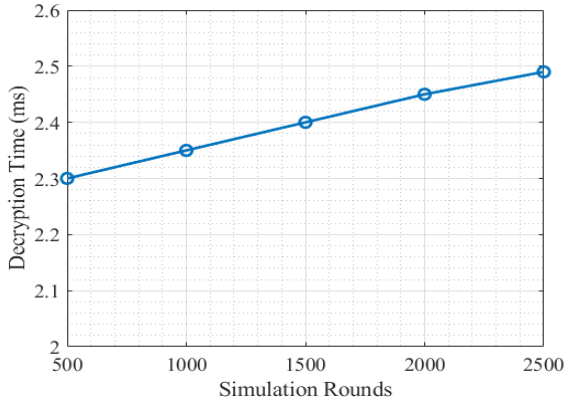

Figure 12 The Decryption Time of the Proposed BbOR-DCNN

4.3. Comparative Analysis

The effectiveness of the BbOR-Deep CNN method is assessed, and its performance is benchmarked against existing techniques to improve data security and privacy with the metrics are accuracy, packet deliver ratio, average energy consumption, data delay, computational complexity, prediction time, encryption time, and decryption time. The existing methods such as DNN, RNN, LSTM, DHMLM [35], CTEER, D2D-MCL, QL-MAC [36], ESECI, ERSS, DbSAEC-HSO, DBDH [37].

4.3.1. Comparison of Proposed Accuracy with Existing Methods

The comparison figure 13 showcases the accuracy of various methods, with DNN achieving 86.43% and RNN improving to 97.81%, demonstrating their sequential data handling capabilities. LSTM further enhances accuracy to 98.49% by preserving long-term dependencies, while DHMLM achieves 99.07% through dynamic hierarchical learning. The proposed BbOR-Deep CNN outperforms all with 99.54% accuracy, leveraging Blockchain, onion routing, and deep CNN for secure communication and effective threat detection. This highlights its superiority over traditional.

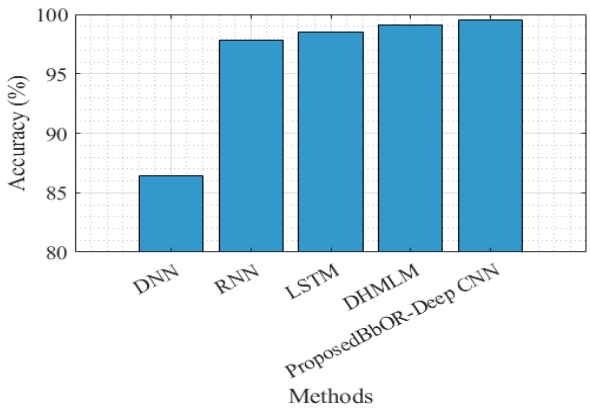

Figure 13 Comparison of Accuracy

4.3.2. Comparison of Proposed Packet Deliver Ratio with Existing Methods

The comparison figure 14 highlights the Packet Delivery Ratio (PDR) performance of four methods CTEER, D2D-MCL, QL-MAC, and the proposed BbOR-Deep CNN across varying simulation rounds. The proposed BbOR-Deep CNN consistently outperforms other methods, demonstrating the highest PDR at all rounds, reaching 92% at 500 rounds and maintaining a robust 92% even at 2500 rounds. In contrast, other methods show a gradual decline in PDR as simulation rounds increase, with CTEER consistently delivering the lowest performance. This indicates the superior reliability and efficiency of the BbOR-Deep CNN method in ensuring high

RESEARCH ARTICLE

PDR over extended simulations. The results validate its effectiveness for secure and reliable communication in dynamic environments.

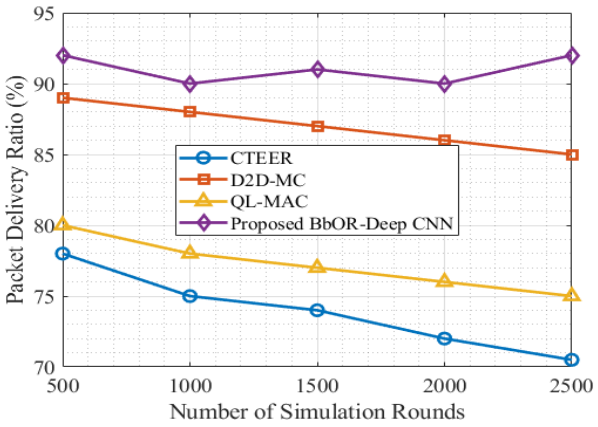

Figure 14 Comparison of PDR

4.3.3. Comparison of Proposed Average Energy Consumption with Existing Methods

Figure 15 compares the average energy consumption of four methods CTEER, D2D-MCL, QL-MAC, and the proposed BbOR-Deep CNN across simulation rounds. At 500 rounds, BbOR-Deep CNN shows the lowest consumption (0.5 J) compared to CTEER (0.9 J), D2D-MCL (0.62 J), and QL-MAC (0.79 J).

As the rounds increase to 2500, BbOR-Deep CNN remains the most efficient at 0.6 J, while CTEER, D2D-MCL, and QL-MAC consume 1.28 J, 0.9 J, and 1.18 J, respectively. The energy consumption of all methods rises with simulation rounds, but BbOR-Deep CNN maintains superior efficiency throughout. This illustrates its ability to achieve significant energy savings while ensuring robust performance.

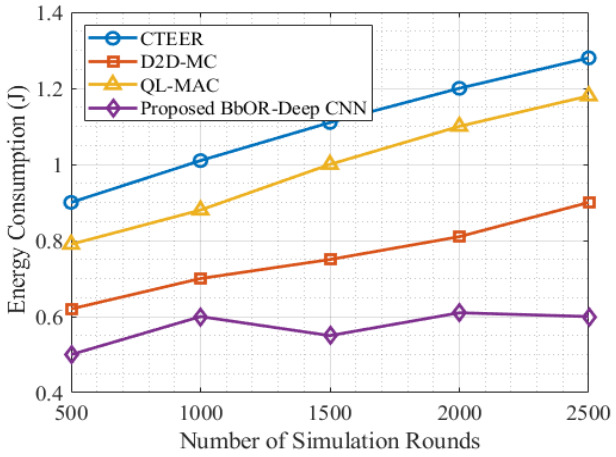

Figure 15 Comparison of Energy Consumption

4.3.4. Comparison of Proposed Data Delay with Existing Methods

The comparison figure 16 shows data delay (in seconds) for various methods across different simulation rounds. In the first round (500 simulations), the proposed BbOR-Deep CNN method achieves a delay of 0.5 seconds, which is significantly lower than CTEER (1.2s), D2D-MCL (0.75s), and QL-MAC (1.09s). As the number of simulation rounds increases, BbOR-Deep CNN continues to maintain the lowest delay, reaching 1 second at 2500 rounds, while other methods experience higher delays. For instance, CTEER's delay increases from 1.2s to 1.45s, D2D-MCL's delay grows from 0.75s to 1.15s, and QL-MAC's delay rises from 1.09s to 1.39s. This demonstrates that BbOR-Deep CNN consistently provides the most efficient performance in terms of minimizing data delay across all simulation rounds.

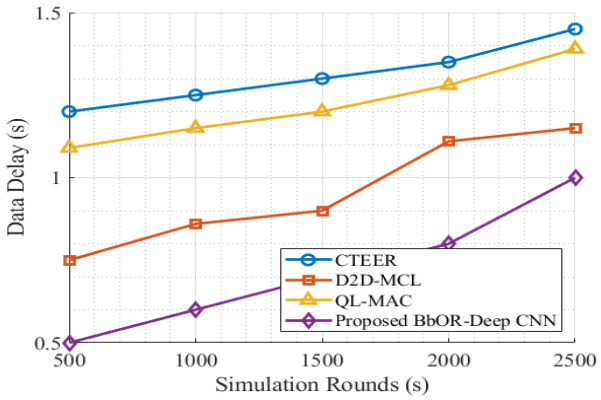

Figure 16 Comparison of Data Delay

4.3.5. Comparison of Proposed Computational Complexity with Existing Methods

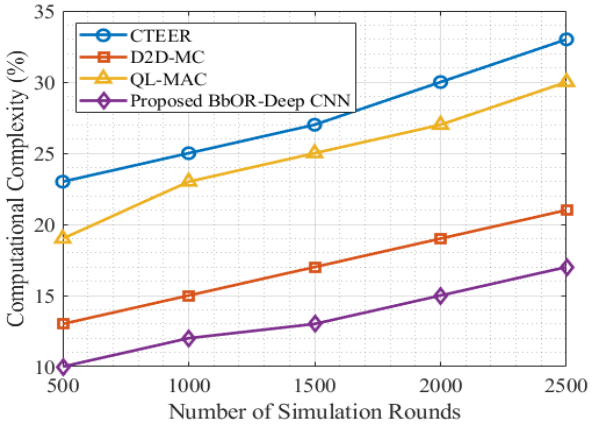

Figure 17 Comparison of Computational Complexity

The comparison figure 17 shows the computational complexity (in percentage) for different methods across

RESEARCH ARTICLE

various simulation rounds. For 500 rounds, the Proposed BbOR-Deep CNN method has a complexity of 10%, significantly lower than CTEER (23%), D2D-MCL (13%), and QL-MAC (19%). As the number of simulation rounds increases to 2500, the complexity for BbOR-Deep CNN rises to 17%, compared to 33% for CTEER, 21% for D2D-MCL, and 30% for QL-MAC. This demonstrates that the Proposed BbOR-Deep CNN consistently maintains lower computational complexity, making it a more efficient and scalable solution across increasing simulation rounds.

4.3.6. Comparison of Proposed Prediction Time with Existing Methods

The comparison figure 18 highlights the prediction time efficiency of various methods, including RNN, DNN, DHMLM, LSTM, and the proposed BbOR-Deep CNN. Among these, the proposed BbOR-Deep CNN demonstrates the lowest prediction time of 12.16 ms, showcasing its superior computational efficiency. Traditional methods such as RNN and LSTM exhibit significantly higher prediction times of 28 and 49.83 ms, respectively, indicating slower processing. While DNN (24.6 ms) and DHMLM (16.3 ms) perform better than RNN and LSTM, they still lag behind the proposed method. This underscores the effectiveness of BbOR-Deep CNN in ensuring rapid and secure predictions in applications requiring real-time performance.

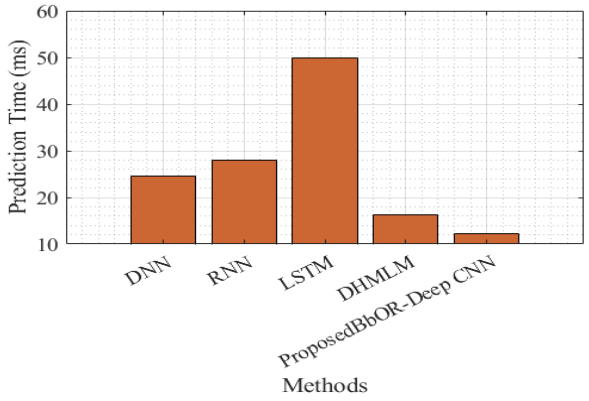

Figure 18 Comparison of Prediction Time

4.3.7. Comparison of Proposed Encryption Time with Existing Methods

The comparison figure 19 highlights the encryption time performance of various methods, showcasing the efficiency of the proposed BbOR-Deep CNN approach. ESECI records the highest encryption time at 70 ms, followed by DbSAEC-HSO at 50 ms, and ERSS at 25 ms. The DBDH method significantly reduces encryption time to 3.55 ms, demonstrating a substantial improvement. However, the proposed BbOR-Deep CNN achieves the fastest encryption time of just 2.31 ms, emphasizing its superior computational efficiency and suitability for real-time applications. This demonstrates the proposed method's ability to optimize encryption processes while ensuring robust security.

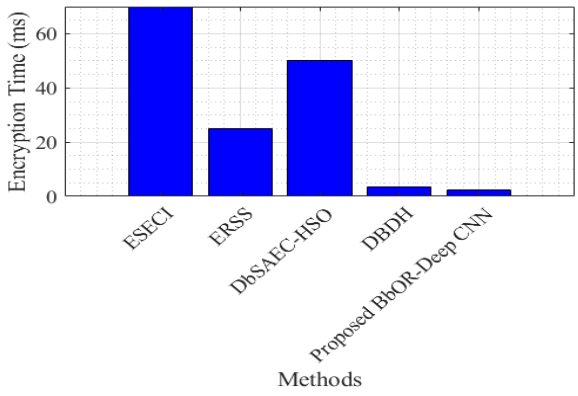

Figure 19 Comparison of Encryption Time

4.3.8. Comparison of Proposed Decryption Time with Existing Methods

The comparison figure 20 highlights the decryption time efficiency of different methods. Among the evaluated approaches, the proposed BbOR-Deep CNN method demonstrates the fastest decryption time at 2.49 ms, significantly outperforming alternatives like DBDH (3.6 ms), DbSAEC_HSO (53 ms), ERSS (35 ms), and ESECI (90 ms).

This performance improvement underscores the effectiveness of the BbOR-Deep CNN's optimized cryptographic and processing framework. The minimal decryption time enhances real-time application suitability, making it highly efficient for secure communication scenarios. This advantage positions BbOR-Deep CNN as a robust solution for time-sensitive security processes.

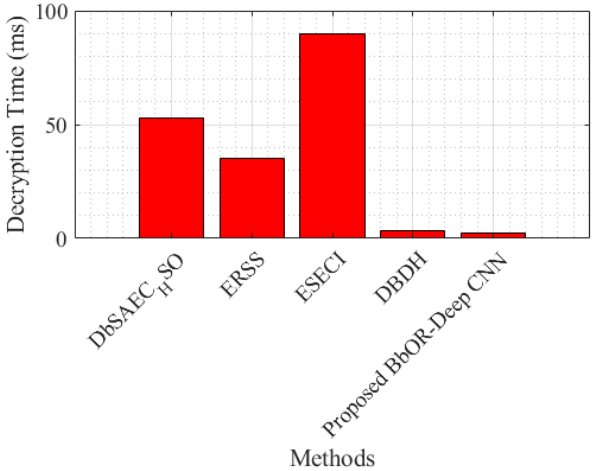

Figure 20 Comparison of Decryption Time

RESEARCH ARTICLE

4.4. Scalability Analysis and Computational Overhead Estimation

The scalability of the proposed BbOR-DCNN framework was analyzed through computational overhead estimation and practical deployment scenarios. The simulation results at 2500 rounds demonstrated that the model maintains high accuracy (99.54%) and security efficiency, with a low computational complexity of 17%, ensuring feasibility in large-scale D2D networks. The packet delivery ratio remains at 92%, while data delay is controlled at 1s, confirming the framework's suitability for real-time applications. Additionally, the deep CNN-based attack detection requires only 12.16ms, making it effective for proactive security in dynamic environments.

To ensure practical deployment, the BbOR-DCNN approach leverages optimized cryptographic token mechanisms, lightweight blockchain consensus, and distributed deep learning for threat detection. These features enable the model to scale efficiently across high-density IoT, smart city, and industrial automation networks without significantly increasing computational overhead. Compared to existing methods, BbOR-DCNN ensures a superior balance between security, efficiency, and scalability, making it a robust solution for securing next-generation D2D communications. Figure 21 illustrates the computational overhead analysis and scalability of the BbOR-DCNN model across different simulation rounds.

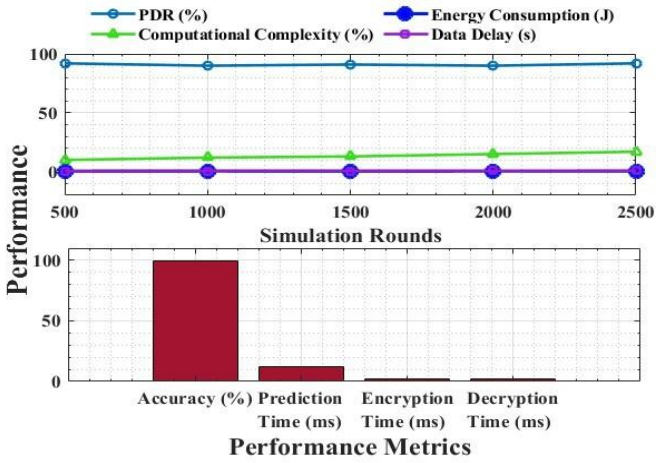

Figure 21 Scalability and Computational Overhead Analysis of the Proposed BbOR-DCNN

4.5. Performance Evaluation of the Proposed Method Before and After Attack Prediction

The proposed method demonstrates remarkable improvements in performance after attack prediction compared to before prediction. Performance evaluation of the proposed method before and after prediction is shown in Table 3. Accuracy significantly increases from 92% to 99.54%, and the PDR improves from 90% to 92%, showcasing enhanced reliability. Energy consumption is reduced from 5.00×10^{-5} J/bit to 0.60 J, indicating better energy efficiency. Data delay decreases from 2.06ms to 1.00ms, and computational complexity improves from 19% to 17%, highlighting faster and more efficient processing. Additionally, encryption and decryption times are notably reduced from 4.85ms to 2.31ms and from 4.91ms to 2.49ms, respectively, while prediction time drops from 13.11ms to 12.16ms. These results underline the effectiveness of the proposed method in enhancing system performance while mitigating attack impacts.

Table 3 Performance Evaluation of the Proposed Method Before and After Prediction

Metric	Before Prediction	After Prediction
Accuracy (%)	92	99.54
Packet Delivery Ratio (%)	90	92
Energy Consumption (Joules/bit)	5.00×10−5	0.60 J
Data Delay (ms)	2.06	1.00
Computational Complexity	19	17
Encryption Time (ms)	4.85	2.31
Decryption Time (ms)	4.91	2.49
Prediction Time (ms)	13.11	12.16

4.6. Statistical Analysis

The statistical analysis of our proposed Blockchain-based Onion Routing with Deep CNN (BbOR-Deep CNN) model validates its performance across key security and efficiency metrics. Table 4 provides the statistical analysis of BbOR-DCNN. The Chi-Square Goodness-of-Fit test ($p = 0.76965$) confirms that the encrypted token distribution is uniform, ensuring consistent encryption across transactions. The Z-Test for Token Validation ($p = 0.41422$) indicates no significant deviation in token validation, reinforcing the robustness of our cryptographic approach. Cohen's Kappa (0.5) demonstrates a moderate agreement in token usage, verifying reliability in secured transactions. The Spearman Correlation ($p = 0.536$) shows no strong correlation between accuracy and prediction time, confirming stable performance irrespective of processing delays. Lastly, the Kruskal-Wallis test ($p = 0.16124$) confirms that PDR remains consistent across

RESEARCH ARTICLE

different simulation rounds, indicating the model's scalability and reliability in real-world deployments. These results collectively demonstrate the model's effectiveness in ensuring secure, efficient, and stable D2D communication.

Table 4 Statistical Analysis of BbOR-Deep CNN Performance Metrics

Statistical Test	P-Value
Chi-Square Goodness-of-Fit for Encryption	0.76965
Z-Test for Token Validation Proportion	0.41422
Cohen's Kappa for Token Usage Agreement	0.5
Spearman Correlation Coefficient (between accuracy and prediction time)	0.536
Kruskal-Wallis Test for PDR Values across Simulations	0.16124

4.7. Discussion

The proposed BbOR-DCNN method achieves superior results due to its integration of multiple advanced security and optimization techniques. Unlike traditional D2D communication methods that suffer from latency, security vulnerabilities, and inefficient attack detection, the proposed approach leverages Blockchain for immutable security, Onion Routing for privacy-preserving transmission, and Deep CNN for proactive attack detection. The combination of these techniques enhances the accuracy (99.54%), and packet delivery ratio (92%), and significantly reduces prediction time (12.16 ms), encryption time (2.31 ms), and decryption time (2.49 ms), making it highly efficient for real-time applications.

Furthermore, the model effectively mitigates adversarial attacks such as Blackhole, Flooding, Grayhole, and TDMA (Scheduling) attacks by employing an intelligent cryptographic token mechanism and anomaly detection through Deep CNN, which continuously learns and adapts to emerging threats. The novel integration of cryptographically secure token authentication with distributed Blockchain validation ensures tamper-proof communication, making the proposed approach scalable, resilient, and ideal for critical applications in IoT, healthcare, and finance. Unlike conventional methods, BbOR-DCNN proactively detects, prevents, and mitigates security threats, ensuring an optimal trade-off between computational complexity (17%) and security robustness. This makes our proposed method not only more efficient but also highly novel in securing D2D communication against evolving cyber threats.

5. CONCLUSION

This research presents an innovative approach to secure and private D2D communication through BbOR-DCNN. The integration of Blockchain ensures trust, transparency, and immutability, while onion routing safeguards communication privacy by anonymizing the transmission path. By incorporating Deep CNN, the system effectively predicts potential attacks using Blockchain transaction patterns and token behaviors, enhancing its security capabilities. The proposed methodology was validated using the WSNDS dataset, demonstrating its scalability and effectiveness in mitigating security risks and preserving data integrity in D2D networks. This framework provides a robust, efficient, and scalable solution suitable for various sensitive applications, including IoT, healthcare, and financial systems. However, the resource-intensive nature of Deep CNN in the framework may challenge its applicability in resource-constrained and real-time environments. To address this, future work will focus on optimizing the BbOR-Deep CNN framework for real-time deployments by leveraging lightweight encryption techniques, efficient Blockchain consensus algorithms, and model compression methods to reduce resource consumption.

REFERENCES

[1] P. Khuntia, and R. Hazra, "An efficient channel and power allocation scheme for D2D enabled cellular communication system: An IoT application," IEEE Sensors Journal, vol. 21, no. 22, pp. 25340-25351, 2021.

[2] P.K. Barik, C. Singhal, and R. Datta, "An efficient data transmission scheme through 5G D2D-enabled relays in wireless sensor networks," Computer Communications, vol. 168, no.1, pp. 102-113, 2021.

[3] I.O. Sanusi, K.M. Nasr, and K. Moessner, "Radio resource management approaches for reliable device-to-device (D2D) communication in wireless industrial applications," IEEE Transactions on cognitive communications and networking, vol. 7, no. 3, pp. 905-916, 2020.

[4] Z. Su, W. Feng, J. Tang, Z. Chen, Y. Fu, N. Zhao, and K.K. Wong, "Energy-efficiency optimization for D2D communications underlaying UAV-assisted industrial IoT networks with SWIPT," IEEE Internet of Things Journal, vol. 10, no. 3, pp. 1990-2002, 2022.

[5] S. Feng, X. Lu, S. Sun, D. Niyato, and E. Hossain, "Securing large-scale d2d networks using covert communication and friendly jamming," IEEE Transactions on Wireless Communications, vol. 23, no. 1, pp. 592-606, 2023.

[6] B. Chang, L. Li, G. Zhao, Z. Chen, and M.A. Imran, "Autonomous D2D transmission scheme in URLLC for real-time wireless control systems," IEEE Transactions on Communications, vol. 69, no. 8, pp. 5546-5558, 2021.

[7] V. Hakami, H. Barghi, S. Mostafavi, and Z. Arefinezhad, "A resource allocation scheme for D2D communications with unknown channel state information," Peer-to-peer networking and applications, vol. 15, no. 2, pp. 1189-1213, 2022.

[8] X. Cai, X. Mo, J. Chen, and J. Xu, "D2D-enabled data sharing for distributed machine learning at the wireless network edge," IEEE Wireless Communications Letters, vol. 9, no. 9, pp. 1457-1461, 2020.

[9] T. Van Nguyen, T.N. Do, V.N.Q. Bao, D.B. da Costa, and B. An, "On the performance of multihop cognitive wireless powered D2D communications in WSNs," IEEE Transactions on Vehicular Technology, vol. 69, no. 3, pp. 2684-2699, 2020.

RESEARCH ARTICLE

[10] M. Pirani., A. Mitra, S. Sundaram, "A survey of graph-theoretic approaches for analyzing the resilience of networked control systems", arXiv preprint arXiv:2205.12498. 2022.
[11] R. Zhang, F.R. Yu, J. Liu, T. Huang, and Y. Liu, "Deep reinforcement learning (DRL)-based device-to-device (D2D) caching with blockchain and mobile edge computing," IEEE Transactions on Wireless Communications, vol. 19, no. 10, pp. 6469-6485, 2020.
[12] R. Zhang, F.R. Yu, J. Liu, R. Xie, and T. Huang, "Blockchain-incentivized D2D and mobile edge caching: A deep reinforcement learning approach," IEEE Network, vol. 34, no. 4, pp. 150-157, 2020.
[13] R. Cheng, Y. Sun, Y. Liu, L. Xia, D. Feng, and M.A. Imran, "Blockchain-empowered federated learning approach for an intelligent and reliable D2D caching scheme," IEEE Internet of Things Journal, vol. 9, no. 11, pp. 7879-7890, 2021.
[14] H. Alghafari, M.S. Haghighi, and A. Jolfaei, "High bandwidth green communication with vehicles by decentralized resource optimization in integrated access backhaul 5G networks," IEEE Transactions on Green Communications and Networking, vol. 6, no. 3, pp. 1438-1447, 2022.
[15] K. Kita, Y. Koizumi, T. Hasegawa, O. Ascigil, and I. Psaras, "Producer anonymity based on onion routing in named data networking," IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 2420-2436, 2020.
[16] J. Pastor-Galindo, F.G. Mármol, and G.M. Pérez, "On the gathering of Tor onion addresses," Future Generation Computer Systems, vol. 145, pp. 12-26, 2023.
[17] De la Cadena, W., Kaiser, D., Mitseva, A., Panchenko, A., Engel, T. "Analysis of multi-path onion routing-based anonymization networks," In Data and Applications Security and Privacy XXXIII: 33rd Annual IFIP WG 11.3 Conference, DBSec 2019, Charleston, SC, USA, July 15–17, 2019, Proceedings 33, pp. 240-258, 2019. Springer International Publishing.
[18] N.K. Jadav, T. Rathod, R. Gupta, S. Tanwar, N. Kumar, R. Iqbal, S. Atalla, H. Mohammad, and S. Al-Rubaye, "Blockchain-based secure and intelligent data dissemination framework for UAVs in battlefield applications," IEEE Communications Standards Magazine, vol. 7, no. 3, pp. 16-23, 2023.
[19] M.H. Zafar, I. Khan, and M.O. Alassafi, "An efficient resource optimization scheme for D2D communication," Digital Communications and Networks, vol. 8, no. 6, pp. 1122-1129, 2022.
[20] A. Allakany, A. Saber, S.M. Mostafa, M. Alsabaan, M.I. Ibrahim, and H. Elwahsh, "Enhancing security in ZigBee wireless sensor networks: A new approach and mutual authentication scheme for D2D communication," Sensors, vol. 23, no. 12, pp. 5703, 2023.
[21] N.K. Jadav, R. Kakkar, H. Mankodiya, R. Gupta, S. Tanwar, S. Agrawal, and R. Sharma, "GRADE: Deep learning and garlic routing-based secure data sharing framework for IIoT beyond 5G," Digital Communications and Networks, vol. 9, no. 2, pp. 422-435, 2023.
[22] F.A. Yaseen, N.A. Alkhalidi, H.S. Al-Raweshidy, "ITor-SDN: Intelligent Tor Networks Based SDN for Data Forwarding Management," IEEE Access, 2023.
[23] S. Liu, G. Yu, D. Wen, X. Chen, M. Bennis, and H. Chen, "Communication and energy efficient decentralized learning over D2D networks," IEEE Transactions on Wireless Communications, vol. 22, no. 12, pp. 9549-9563, 2023.
[24] D. Yang, S. Yoo, I. Doh, and K. Chae, "Selective blockchain system for secure and efficient D2D communication," Journal of Network and Computer Applications, vol. 173, no. 1. pp. 102-817, 2021.
[25] L. Luo, Z. Liu, Z. Chen, M. Hua, W. Li, and B. Xia, "Age of information-based scheduling for wireless D2D systems with a deep learning approach," IEEE Transactions on Green Communications and Networking, vol. 6, no. 3, pp. 1875-1888, 2022.
[26] S.H. Park, T. Mahboob, S.T. Shah, M.A. Shawky, M. Choi, and M.Y. Chung, "Blockchain-assisted Dynamic Resource Pool Selection for D2D Roaming Scenarios," IEEE Open Journal of the Communications Society, 2024.
[27] J. Miao, Z. Wang, X. Xue, M. Wang, J. Lv, and M. Li, "Lightweight and secure D2D group communication for wireless IoT," Frontiers in Physics, Vol. 11, no.1, pp. 1210777, 2023.
[28] J. Kiran, et al. "Enhancing Secure Data Transfer in Wireless Networks Using Onion Routing and Blockchain Technology." 2024 Global Conference on Communications and Information Technologies (GCCIT). IEEE, 2024. pp. 1-6, doi: 10.1109 / GCCIT63234.2024.10862069.
[29] J, K.B., Nigam, M.K. and Shinde, S.B. A Hybrid Framework for Secure Device-To-Device Communication in Wireless Systems Using Blockchain and Onion Routing. ShodhKosh: Journal of Visual and Performing Arts. 5, 1 (Jun. 2024), 2269–2277.
[30] L. Almuqren, K. Mahmood, S.S. Aljameel, A.S. Salama, G.P. Mohammed, and A.A. Alneil, "Blockchain Assisted Secure Smart Home Network using Gradient Based Optimizer with Hybrid Deep Learning Model," IEEE Access 11 (2023): 86999-87008.
[31] R.A. Chavan, "Cloud Data Security Improvement Using Cryptographic Steganography by Truly Random and Cryptographically Secure Random Number," (Doctoral dissertation, Dublin, National College of Ireland), 2023.
[32] S. Schlor, R. Strässer, and F. Allgöwer, "Koopman interpretation and analysis of a public-key cryptosystem: Diffie-Hellman key exchange," IFAC-PapersOnLine, vol. 56, no. 2, pp. 984-990, 2023.
[33] R. Gupta, S. Tanwar, and N. Kumar, "B-IoMV: Blockchain-based onion routing protocol for D2D communication in an IoMV environment beyond 5G", Vehicular Communications, vol. 33, no. 1. p.100401, 2022.
[34] M.J. Pasha, K.P. Rao, A. MallaReddy, and V. Bande, "LRDADF: An AI-enabled framework for detecting low-rate DDoS attacks in cloud computing environments", Measurement: Sensors, 28, p.100828, 2023.
[35] S.J. Rani, I.I. Ioannou, P. Nagaradjane, C. Christophorou, V. Vassiliou, H. Yarramsetti, S. Shridhar, L.M. Balaji, and A. Pitsillides, "A novel deep hierarchical machine learning approach for identification of known and unknown multiple security attacks in a d2d communications network", IEEE Access, vol. 11, no.1, pp.95161-95194, 2023.
[36] K. Haseeb, A. Rehman, T. Saba, S.A. Bahaj, and J. Lloret, Device-to-device (D2D) multi-criteria learning algorithm using secured sensors. Sensors, Vol. 22, no. 6, p.2115, 2022.
[37] A. Goel, and S. Neduncheliyan, "An intelligent blockchain strategy for decentralized healthcare framework", Peer-to-Peer Networking and Applications, vol. 16, no. 2, pp.846-857.

Authors

Kiran Jadhav have pursued B.E. & M.E. degree from North Maharashtra university, Jalgaon, Maharashtra, India And pursuing Ph.D. from Kalinga University, Raipur, Chhattisgarh, India. His research interest area is Wireless Sensor Network, Communication Systems, IoT and Cloud Computing.

Dr. Manoj Kumar Nigam has more than 20 years of experience in teaching and research. He is Professor at Kalinga University, Raipur, Chhattisgarh, India. His current research focuses on Distributed generation, power Electronics drives and power quality Issues in the Power System. He has published more than 30 research papers in scopus indexed journal and conferences.

RESEARCH ARTICLE

Dr. Sagar Shinde is working as a Professor in Computer Science Engineering – Artificial Inteligence department at Nutan Maharashtra Institute of Engineeirng & Technology, Pune, India. He has 15.5 years of experience in teaching and research. His current research focus is on Soft Comuputing and Artificial Intelligence. He has published more than 35 research papers in scopus indexed journals and conferences.

Dr. Lalitkumar Wadhwa is working as a Dean at Ajeenkya DY Patil University, Lohegaon, Pune, Maharashtra, India. He has 25 years of experience in teaching and research. His area of specialization is Communication Systems & Wireless Sensor Networks. He has published more than 20 research papers in Scopus-indexed journals and conferences.

Dr. Pramod Patil is working as a Dean – Research And Developement at Dr. D. Y. Patil Institute of Technology, Pimpri, Pune, India. He has 24 years of experience in teaching and research. His area of specialization is Artificial Inteligence & Soft Computing. He has published more than 50 research papers in scopus indexed journals and conferences.

How to cite this article:

Kiran Bhavlal Jadhav, Manoj Kumar Nigam, Sagar Bhilaji Shinde, Lalitkumar Wadhwa, Pramod Patil, “Device-to-Device (D2D) Wireless Communication Using Blockchain and Onion Routing”, International Journal of Computer Networks and Applications (IJCNA), 12(2), PP: 208-226, 2025, DOI: 10.22247/ijcna/2025/14.