



ISSN ONLINE: 2447-0228



## RESEARCH ARTICLE

## OPEN ACCESS

# XTREME GRADIENT BALLOON CRYPTOGRAPHIC COMPRESSED BLOCKCHAIN BASED SECURE ROUTING IN COGNITIVE RADIO NETWORK

T. Sundar<sup>\*1</sup>, A. Senthilkumar<sup>2</sup>

<sup>1</sup>Ph.D. - Research Scholar, Department of Computer Science, Periyar University, Salem, India.

<sup>2</sup>Assistant professor, Department of Computer Science, Thiruvalluvar Government Arts College, Rasipuram, India.

<sup>1</sup><http://orcid.org/0000-0003-2788-5884>, <sup>2</sup><http://orcid.org/0000-0002-9420-7605>

E-mail: \*[admin.sundar@gmail.com](mailto:admin.sundar@gmail.com), [senthilkumarmca76@gmail.com](mailto:senthilkumarmca76@gmail.com)

## ARTICLE INFO

### Article History

Received on: January 03, 2026

Reviewed on: February 08, 2026

Accepted on: July 01, 2026

Published on: July 31, 2026

### Keywords:

Cognitive Radio Networks,  
Quality Of Service,  
Extreme Gradient Boost\Quadratic  
Node Classifier,  
Balloon Cryptographic,  
Matyas–Meyer–Oseas Block  
Compression.

## ABSTRACT

The inception of cognitive radio networks (CRNs) institutes both possibilities and complications in spectrum access and security. Blockchain technology has made an appearance as a possible solution to address these issues, providing improved transparency, security and effectiveness in spectrum management. Researchers propose several security methods to mitigate these attacks, each with drawbacks. Most of these methods have higher complexity, while others cannot be used to focus on training time and accuracy. To overcome these issues while maintaining higher security and Quality of Service (QoS), a novel blockchain method called, eXtreme Gradient Boost Quadratic Balloon Cryptographic Block Compression (XGBQ-BCBC) based secured routing in CRN is proposed. The method initially collects multiple secondary user and primary user from different cognitive radio controllers and creates blocks for the storage of these sets in blockchain network. Here, the eXtreme Gradient Boost Quadratic Node Classifier is employed where the weak classifier results are combined using Quadratic Classifier for classifying and authenticating the nodes as normal nodes or attacks based on the residual energy and relative trustworthiness factor and stored in the blockchain. At this point, the data packets collected from the normal nodes are hashed by using Balloon Cryptographic Matyas–Meyer–Oseas (MMO) Block compression function. Next, the hashed results are sent to the normal nodes by authenticating the normal nodes. If normal node's authentication verification is passed, then the hashed results are said to the receiver nodes, therefore ensuring robust data transmission in the CRN. The simulation results of the proposed method demonstrate 27%, 32% data confidentiality and data integrity in the presence of MUs, when compared to other methods like Channel Availability Probability and multi-objective optimization. As a result the security of cognitive radio blockchain network is demonstrated to be improved in a significant manner.



Copyright ©2026 by authors and Galileo Institute of Technology and Education of the Amazon (ITEGAM). This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

## I. INTRODUCTION

A robust routing path was identified in [1] by reducing the PU interference and routing delay to increase the throughput within IIoT domain. A generic routing framework was introduced from cross-layer perspective to share information resources based on Channel Availability Probability. A novel cross-layer-oriented routing protocol was introduced using time-variant channel estimation technique. The designed protocol periodically updated and stored routing table information for optimal route decision-making. A new routing metric was used to achieve higher throughput and lower delay. Though the throughput was improved, the computational cost was not minimized by robust routing path. A spectrum allocation strategy was introduced in [2] with cognitive radio (CR) technology. The time-sensitive and regular communication service requirements were addressed with distribution terminal communication services for power quality monitoring with secondary data (SD).

An optimization problem was addressed with indicators like SD transmission rate and maximum latency. The convex optimization method was used to attain optimal power and frequency bandwidth allocation for users with SD. However, the computational complexity was not reduced by spectrum allocation strategy. Blockchain-based technology was introduced in [3] to detect and prevent criminal activities. The designed technology employed blockchain-based malicious user detection with SHA-3 hashing and energy detection-based Spectrum sensing. The detection strategy comprised block updating phase and iron out phase. But, the data confidentiality was not at required level. A blockchain-based smart contracts was introduced in [4] with blockchain for making transactions private among participants. The blockchain measured trustworthiness of particular user depending on accuracy level of sensing results. A money locking approach was introduced where the penalty gets deducted. But the routing time was not reduced by blockchain-based smart contracts. Two novel blockchain-based methods that took into considerations multiple input multiple outputs in a single cell network to boost the overall performance were presented in [5]. Energy-efficiency and security was provided in [6] using blockchain enabled clustering mechanism contributing to sustainable development. A Multi-Level Trust Based Secure Routing was proposed in [7] to improve overall QoS performance. Blockchain technology (BCT) materializes as a notable player in boosting the spectrum access security.

Also the fusion of blockchain and 6G results in increased security. Combining blockchain with IoT systems improves security by encrypting and digitally signing IoT data as blockchain transactions. To improve spectrum utilization efficiency, node evaluation and selection algorithm were proposed in [8] therefore improving the network security against malicious node attacks. A review of accessing spectrum in dynamic fashion with blockchain architecture was presented in [9]. Significant contribution and developments by combining blockchain with CRN was investigated in [10]. A comprehensive review covering security threats along with mitigation mechanisms for industrial IoT was provided in [11]. Different security challenges in addition to security integration for establishing security were presented in [12]. In spite of the significant research efforts, a lack in comprehensive survey still is said to exist. A state-of-the-art blockchain based trust and reputation based mechanisms were presented in [13]. A complete review on dynamic access of spectrum with blockchain was presented in [14]. A holistic and systematic survey was presented in [15] to meet the requirement of blockchain. Overall, the paper provides a complete overview of the work accomplished, concentrating on the integration of deep learning, blockchain technology and cryptographic mechanism to address the security issues CRNs. The proposed method exhibits the performance metric improvements and exhibits its prospective as an efficient solution for improving security and real-time protection in CRNs.

## 1.1 MOTIVATION

The motivation of this work is to address the security issues encountered by CRNs. Combining the adaptability of blockchains with the intelligence of cognitive radios CRNs validate dynamic and effective communication in a variety of scenarios. However, these networks are susceptible to a variety of authentication issues. Existing deep learning method modeled to address these security aspects, however suffer from secure routing and an absence of proper node authentication mechanism.

## 1.2 CONTRIBUTIONS

This work contributes the following to addressing aforementioned issues employing eXtreme Gradient Boost Quadratic Balloon Cryptographic Block Compression (XGBQ-BCBC) based secured routing in CRN.

- To present a novel secure data routing method that employs eXtreme Gradient Boost Quadratic Node Classifier to classify between normal nodes and malicious nodes based on residual energy and relative trustworthiness factors. This strategy improves ability to authenticate users in a computationally and accurate manner.
- To store the analyzed data packets on a blockchain-based distributed network in order to ensure data integrity and data confidentiality.
- The blockchain implementation in the proposed method employs a Balloon Cryptographic Matyas–Meyer–Oseas (MMO) Block compression-based Secure Routing. This model ensures the integrity and confidentiality of the stored data packet, thereby boosting the method's overall security.
- Compared to existing methods, the blockchain-based security method called, eXtreme Gradient Boost Quadratic Balloon Cryptographic Block Compression (XGBQ-BCBC) in CRN demonstrates significant performance enhancements in a number of performance metrics. The proposed method achieves a remarkable reduction in authentication time (x% and y% relative to Channel Availability Probability and multi-objective optimization respectively), improves data confidentiality (x% and y% relative to the same models), increase data integrity (x% and y% relative to the same models) during various communications. These improvements contribute to the security and efficiency of CRNs as a whole.

## 1.3 ORGANIZATION OF THE WORK

The remaining of the paper is organized as follows. The background of CRN and blockchain based secure routing in CRN for data confidentiality and data integrity is explained in section 2 with the reviews of related work discussed in detail. Section 3 explains the system model followed by which the proposed method, XGBQ-BCBC is elaborated using diagram and algorithmic description. Case study and inferences are provided in Section 4 with the experimental setup, results and discussion analyzed in section 5 and 6. Finally, section 6 concludes the paper.

## II. RELATED WORKS

Cognitive Radio Networks (CRNs) are under sustained attacks from compromised primary and secondary users. Researchers propose several security mechanisms to circumvent these attacks, each with drawbacks.

Most of these methods have higher complexity and in contrast cannot be utilized to take the edge off multiple attack types. To overcome these drawbacks while sustaining higher security and Quality of Service (QoS) under attacks, a novel blockchain-based security method for boosting attack resilience in CRNs was proposed in [16]. The method showcased higher throughput with higher packet delivery ratio for several real-time cognitive radio scenarios. Nevertheless, CRN could result in considerable security issues while not focusing on privacy attacks during Spectrum Sensing (SS). A pareto encryption standard along with fine tunable recurrent neural network was presented in [17] to ensure privacy preservation. Yet another method to improve communication employing decentralized blockchain was proposed in [18] for improving integrity level. CRNs integrate features of ad-hoc networks with cognitive radios to ease a variety of communication scenarios. Nevertheless, these CRNs are governed by uninterrupted attacks both from internal and external adversaries. They provide a trustworthy platform to deal with security, privacy, scalability and so on. Woefully, the attackers can still inoculate traffic to hinder blockchain nodes systematic functionalities. An optimized Blockchain-based IoT architecture was presented in [19] to attain optimized throughput therefore achieving efficacy extensively. Moreover, their constrained IP tracing potentialities make them inappropriate for real-time scenarios. To address this aspect, a novel blockchain-based method for deep traffic pattern analysis and circumventing of malicious attacks in CRNs was presented in [20]. Yet another framework employing blockchain technology to identify malicious users accurately was designed in [21]. A two-level shared key authentication mechanism with the aid of channel state information and DL was presented in [22] with high secrecy.

Light-weight convolutional neural network was employed in [23] to address on three different aspects, spectrum sensing, data routing and secure transmission based on the adaptive intelligent behavior. Yet another security mechanism employing federated learning was designed in [24] to confirm robustness. A holistic review on designing privacy-preserving reputation mechanism for IoT applications was investigated in [25]. Yet another blockchain framework to ensure transparency and security was presented in [26]. Generate of hash function was employed in [27] for blockchain transaction with improved accuracy. Conventional routing mechanisms frequently lack in imparting adequate security, resulting in data breaches. To address this issue, a greedy routing protocol with blockchain as infrastructure was presented in [28]. By employing greedy forwarding mechanism security was enhanced along with reliable data transmission. A blockchain-based cyber security mechanism employing machine learning was proposed in [29] along with a detailed review. Yet another optimal and secure routing using deep learning in [30] with minimal interference level and strong security during routing. From the scrutiny of related works, restricted conventional deep learning solutions have been designed to measure the effectiveness of secure routing in CRN. Instead of focusing on entire numbers of users, by splitting them into normal and malicious users via blockchain, results in minimizing the end-to-end delay with improved authentication accuracy. With this objective a novel method called, eXtreme Gradient Boost Quadratic Balloon Cryptographic Block Compression (XGBQ-BCBC) based secured routing in CRN is proposed. The elaborate description of the XGBQ-BCBC method is provided in the following sub-sections.

### III. EXTREME GRADIENT BOOST QUADRATIC BALLOON CRYPTOGRAPHIC BLOCK COMPRESSION (XGBQ-BCBC) BASED SECURED ROUTING IN CRN

Many of these methods are characterized by high complexity that may results in challenges in implementation or performance efficiency. Some methods are specialized to address on the authenticity but might not be versatile enough to reduce the training time. This could leave the network vulnerable to unaddressed authentication. In response to the identified drawbacks, the paragraph introduces a novel blockchain-based security method called, eXtreme Gradient Boost Quadratic Balloon Cryptographic Block Compression (XGBQ-BCBC) in CRN. The method's is outlined with several key features:

#### III.1 BLOCKCHAIN-BASED CRN SYSTEM MODEL

Figure 1 show the system model for blockchain-based secured routing in Cognitive Radio Network (CRN) with 'u' secondary users 'SUs' and a primary user 'PU'.

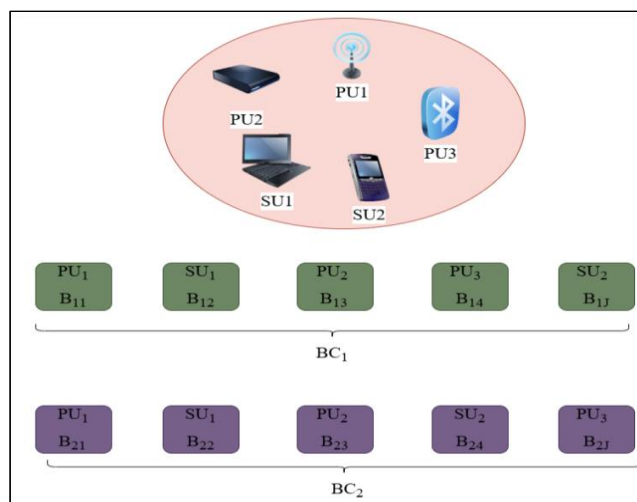


Figure 1: Blockchain-based CRN System Model.  
Source: Authors, (2026).

Moreover, there may be ' $v$ ' malicious users ' $MUs$ ' in the spectrum sensing to degrade network performance. The act of spectrum sensing is performed by secondary users ' $SUs$ ' and broadcast the local decisions to all other adjacent users with updates in the blocks ' $B_t$ ' for time duration ' $t$ '. Hence, new blocks are created after every ' $\tau$ ' units of time and get chained, therefore forming a blockchain. In this manner, blocks are created for primary user ' $PU$ ' and secondary users ' $SUs$ ' therefore forming blockchain for further processing. Also, secure routing in blockchain-based networks consists of functions involving control plane and data plane. As far as control plane is concerned routing decisions are made and validated utilizing blockchain technology and on the other hand, the data plane is responsible for actual secure forwarding of data packets on the basis of rules determined by control plane.

### III.1.1 Registration

In the proposed method, number of cognitive users or nodes is collected as an input. Initially, the primary user ' $PU$ ' and secondary user ' $SU$ ' are registered in the blockchain for performing secure data management in cognitive radio network (CRN). This is explained as given below.

### III.1.2 Primary User and Secondary User Registration Process

Here, initially the number of primary user ' $PU$ ' is registered in the blockchain by utilizing their User ID and Network ID. This is mathematically represented as given below.

$$Reg_a^{PU} = [Reg_1^{PU} + Reg_2^{PU} + \dots + Reg_m^{PU}], \text{ where } a = 1, 2, \dots, m \quad (1)$$

From the above equation (1), ' $a = 1, 2, \dots, m$ ' denotes the number of registered primary user ' $PU$ ' and ' $(Reg_1^{PU})$ ' denoting the first registered primary user ' $PU$ '. In a similar manner, the number of secondary user ' $SU$ ' is registered and is mathematically represented as given below.

$$Reg_b^{SU} = [Reg_1^{SU} + Reg_2^{SU} + \dots + Reg_n^{SU}], \text{ where } b = 1, 2, \dots, n \quad (2)$$

From the above equation (2), ' $b = 1, 2, \dots, n$ ' denote the number of registered secondary user ' $SU$ ' with ' $Reg_n^{SU}$ ' representing the ' $n - th$ ' registered secondary user in blockchain.

### III.1.3 Extreme Gradient Boost Quadratic Node Classifier

The eXtreme Gradient Boost Node Classifier employed in our work denotes a scalable tree optimization with the boosting concept being the root of classifier combines the forecasting of weak learners (i.e. Quadratic classifier) with additive training methods to develop a strong learner. Moreover, by combining the weak quadratic classifier results to that of the strong eXtreme Gradient Boost Node Classifier results aids in avoiding overfitting and enhances mathematical ability. The eXtreme Gradient Boost Node Classifier along with Quadratic classifier is illustrated in figure 2.

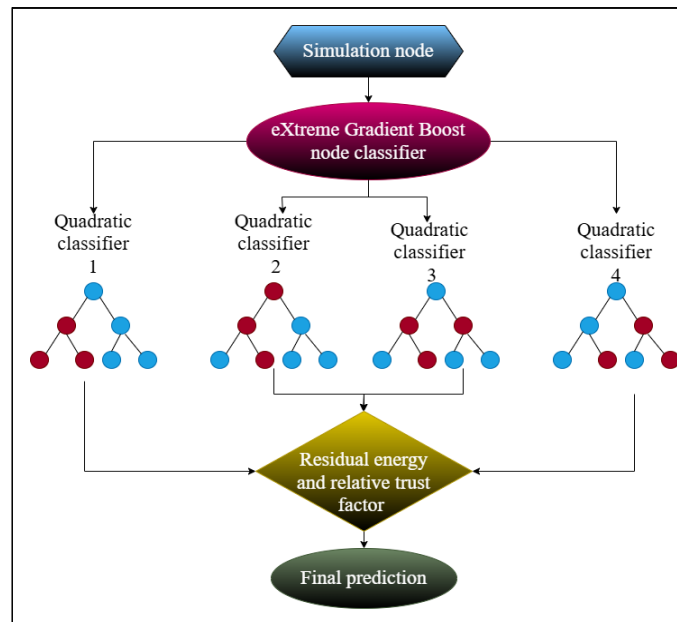


Figure 2: Structure of eXtreme Gradient Boost Quadratic Node Classifier.

Source: Authors, (2026).

From the above figure the objective functions (i.e. normal and malicious node classification based on the residual energy and relative trustworthiness) are simplified by allowing the prediction and regularization terms to be combined. The mathematical formulate is as given below.

$$x_i = f_i^{(k)} = \sum_{l=1}^k f_l(SU_i[E_{Res}(t), RT]) = f_i^{(k-1)} + f_k(SU_i[E_{Res}(t), RT]) \quad (3)$$

From the above equation (3) ' $f_k(SU_i[E_{Res}(t), RT])$ ' denotes the learner at step ' $k$ ', ' $f_i^{(k)}$ ' denotes the prediction at ' $k$ ', ' $f_i^{(k-1)}$ ' represent the prediction at ' $k-1$ ' with respect to the input features ' $f_k(SU_i[E_{Res}(t), RT])$ ' with high residual energy and relative trust factor for the corresponding secondary user respectively. Following which the Quadratic Classifier is formulated as given below by means of likelihood ratio (LR).

$$LR = \frac{\sqrt{2\pi|\Sigma_1|}^{-1} \exp\left(-\frac{1}{2}(x-\mu_1)^T \Sigma_1^{-1}(x-\mu_1)\right)}{\sqrt{2\pi|\Sigma_0|}^{-1} \exp\left(-\frac{1}{2}(x-\mu_0)^T \Sigma_0^{-1}(x-\mu_0)\right)} \quad (4)$$

From the above equation (4), the likelihood ratio ' $LR$ ' value is arrived at based on the means ' $\mu_1, \mu_0$ ', covariance matrices ' $\Sigma_1, \Sigma_0$ ', corresponding to ' $LR = 0$ , when the secondary user is normal node', ' $LR = 1$ , when the secondary user is malicious node' respectively. These values are sent in to the boosted eXtreme Gradient Boost Node Classifier to generate the final results.

### III.1.4 Residual Energy Calculation

Primary Users being licensed owners of a specific spectrum band are assumed to have guaranteed access and does not depend on opportunistic spectrum access or residual energy calculations. On the other hand Secondary Users are unlicensed that possessing limited power sources necessitates residual energy evaluation. In CRN the unlicensed secondary users can opportunistically utilize spectrum bands that are not being utilized by licensed primary users. However, upon detection of a primary user's signal the secondary users must vacate the channel immediately. Hence, based on the residual energy and trust value, the nodes are categorized using eXtreme Gradient Boost Node Classifier. Here, the eXtreme Gradient Boost Node Classifier combines the weak classifier result to attain strong classifier output. Quadratic Classifier is taken as weak classifier for classifying and authenticating nodes as normal nodes or malicious nodes. By combining the weak classifier results, classification performance gets improved. The residual energy of a node in Cognitive Radio Network (CRN) is the amount of energy remaining after a certain time instance, taking into consideration the energy consumed while performing several operations like, transmission, reception and idle states. The mathematical formula for measuring residual energy at time instance ' $t$ ' for each registered secondary user is calculated as given below.

$$E_{Res}(t) = Reg_b^{SU} \text{Max} (E_{Init} - [E_{Trans}(t) + E_{Recv}(t) + E_{Idle}(t)]) \quad (5)$$

From the above equation (5) the residual energy ' $E_{Res}(t)$ ' is measured by considering the values of energy consumed while transmitting data packets ' $E_{Trans}(t)$ ' at time ' $t$ ', energy consumed while receiving data packets ' $E_{Recv}(t)$ ' and energy consumed during the idle stage ' $E_{Idle}(t)$ ' respectively. Higher the measured residual energy result of the registered secondary user higher is the probability of secondary user being normal node.

### III.1.5 Relative Trustworthiness Calculation

Relative trustworthiness of a user in CRN is formulated based on the distance factor for each registered secondary user as given below.

$$RT = Reg_b^{SU} \text{Max} \left[ \min \left( \frac{Dis_1}{Dis_2}, \frac{Dis_2}{Dis_1} \right) \right] \quad (6)$$

From the above equation (6) relative trustworthiness ' $RT$ ' factor is arrived at based on the minimum distance between users. Higher the relative trustworthiness of the registered secondary user higher is the probability of secondary user being normal node. The distance factor is measured as given below.

$$Dis_1 = \sqrt{(P_{SU_i} - P_{PU})^2 + (Q_{SU_i} - Q_{PU})^2} \quad (7)$$

$$Dis_2 = \sqrt{(P_{MU} - P_{SU_i})^2 + (Q_{MU} - Q_{SU_i})^2} \quad (8)$$

From the above equations (7) and (8), ' $(P_{SU_i}, Q_{SU_i})$ ' represents the ' $P$ ' and ' $Q$ ' coordinates of ' $i$ -th' secondary user ' $SU$ ', ' $(P_{PU}, Q_{PU})$ ' denoting ' $P$ ' and ' $Q$ ' coordinates of primary user and ' $(P_{MU}, Q_{MU})$ ' referring to the ' $P$ ' and ' $Q$ ' coordinates of malicious user respectively. To make the overfitting rational while minimizing the methods speed the mathematical formula to evaluate the goodness for original function is as given below.

$$\text{Objective}^{(p)} = \sum_{l=1}^n \mathcal{L}(Res_i - Res'_i) \quad (9)$$

From the above equation (8), ' $\mathcal{L}$ ', denotes the loss function for the corresponding ' $n$ ' number of observations employing Lasso regularization term represented as given below.

$$\mathcal{L} = \sum_{i=1}^n Res_i - (x_i \beta)^2 + \sum_{j=1}^m |\beta_j| \quad (10)$$

From the above loss function results (9) are arrived at based on the actual result ' $Res_i$ ', predicted results ' $Res'_i$ ' for the corresponding input ' $x_i$ ' with respect to a coefficient value ' $\beta$ ' respectively. The pseudo code representation of eXtreme Gradient Boost Quadratic Node Classifier is given below.

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Input:</b> Primary Users ' $PU = PU_1, PU_2, \dots, PU_m$ ', Secondary Users ' $SU = SU_1, SU_2, \dots, SU_n$ '                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Output:</b> Computationally-efficient authentication                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Step 1: <b>Initialize</b> ' $m$ ', ' $n$ '<br>Step 2: <b>Begin</b><br>Sep 3: <b>For</b> each Primary Users ' $PU$ ', Secondary Users ' $SU$ '<br>Step 4: Perform primary user and secondary user registration according to (1) and (2)<br>Step 5: Generate extreme boosting and quadratic classifier results according to (3) and (4)<br>Step 6: Evaluate residual energy according to (5)<br>Step 7: Evaluate relative trustworthiness results according to (6), (7) and (8)<br>Step 8: Evaluate the goodness for original function according to (9) and (10)<br>Step 9: Generate results of malicious nodes ' $MN$ ' and normal nodes ' $NN$ '<br>Step 10: Return node classified results (normal nodes ' $NN$ ' along with data packets ' $DP$ ')<br>Step 11: <b>End for</b><br>Step 12: <b>End</b> |

Algorithm 1: eXtreme Gradient Boost Quadratic Node Classifier.

Source: Authors, (2026).

As given in the above algorithm initially the registered primary user and secondary user are generated in the form of block. Following which only the registered users in the block undergo the process of classification. With the utilization of eXtreme Gradient Boost Node Classifier (i.e. strong learner) and Quadratic Classifier (i.e. weak learner) for node classification process combines the prediction results from several weak learners. With the aid of several weak learners each new tree correct the errors made by the previous tree, resulting in a highly accurate result. Also, by selecting the nodes with high residual energy and relative trustworthiness as basis in turn minimizes the overall time consumed in actual authentication process.

### III.2 BALLOON CRYPTOGRAPHIC MATYAS–MEYER–OSEAS (MMO) BLOCK COMPRESSION-BASED SECURE ROUTING

Second, data packets are collected from normal nodes for ensuring secured routing. In our work, Balloon Cryptographic hash-based Matyas–Meyer–Oseas (MMO) compression is applied for ensuring secured data routing. Figure 3 shows the structure of Balloon Cryptographic Matyas–Meyer–Oseas Block compression model.

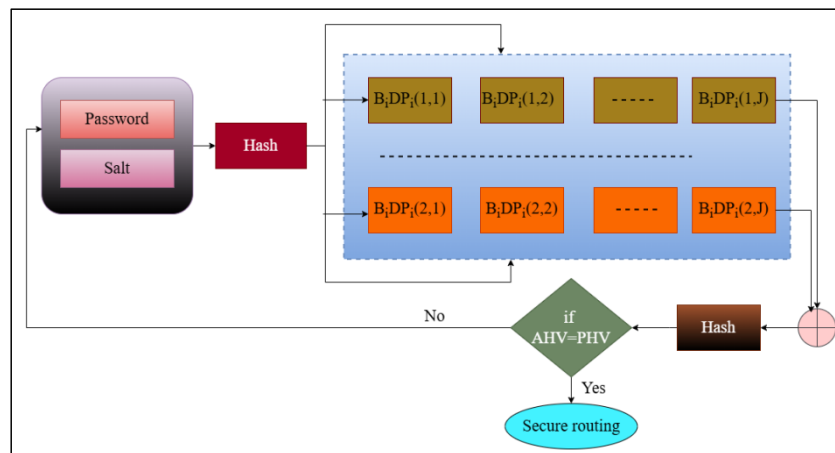


Figure 3: Structure of Balloon Cryptographic Matyas–Meyer–Oseas Block compression model for secure routing in CRN.

Source: Authors, (2026).

As shown in the above figure, the normal nodes sensed data packets are provided as input. The scenario described, involves the utilization of Balloon Cryptographic hash function for secured data routing and Matyas–Meyer–Oseas (MMO) compression function for hash generation in a blockchain control plane with blockchain as basic architecture. The function generates hash value for every normal nodes sensed data packets using Matyas–Meyer–Oseas Compression Function. Moreover, the hash value generation is considered as an encryption process for every data packets. This is performed via expansion, mixing and output hash generation. The hashed data are sent to the source node. The decryption process is carried out in the destination node to obtain original data, therefore preventing illegal access. This guarantees the secured data routing in CRN. The Matyas–Meyer–Oseas Compression function is one of the typical mechanisms in building a single-block-length compression function from a block cipher. The function ' $f$ ' obtains an input chaining value ' $H_{i-1}$ ' along with data packet block ' $DP_i$ ' to generate next chaining value ' $H_i$ ' employing a block cipher ' $E$ '. This is mathematically formulated as given below.

$$H_i = E_{H_{i-1}}(DP_i) \oplus DP_i \quad (11)$$

From the above equation (11), the previous has value ' $H_{i-1}$ ' represents the block cipher key value for the corresponding plain text (i.e., data packet ' $DP_i$ ') with the output ' $H_i$ ' forming the XOR ' $\oplus$ ' of the cipher text ' $E_{H_{i-1}}(DP_i)$ ' and plain text ' $DP_i$ ' respectively.

### III.2.1 Expansion

In the expansion stage, to start with large buffer of memory is filled with a pseudorandom byte sequence ' $PRBseq$ '. This pseudorandom byte sequence ' $PRBseq$ ' is arrived by repeatedly hashing a fusion of the password ' $Pwd$ ' and salt ' $St$ ' provided as inputs to the function. This is mathematically formulated as given below.

$$IV = DP_i[PRBseq + H(Pwd + St)] \quad (12)$$

From the above equation (12) the input value is generated based on the pseudorandom byte sequence ' $PRBseq$ ', along with user provided data ' $Pwd$ ' and arbitrary piece of data ' $St$ ' for each normal nodes sensed data packets ' $DP_i$ ' respectively.

### III.2.2 Mixing

Following which in the mixing stage, the bytes within the allocated memory buffer for each input value ' $IV$ ' are mixed repeatedly for a specified number of iteration. In each iterations' a block in the buffer is updated by hashing its current value, value of the previous block and values from other arbitrarily selected blocks within the buffer. This is mathematically formulated as given below.

$$B_i DP_i = H_i[B_i] + H_{i-1}[B_{i-1}] + \dots + H_m[B_m]_{iter} \quad (13)$$

From the above equation (13) for each block ' $B_i$ ' with corresponding normal sensed nodes data packets ' $DP_i$ ', mixing operation is performed repeatedly overall several iterations ' $iter$ ' with the results of the Matyas–Meyer–Oseas Compression function deciding the memory locations to access. Finally upon successful completion of the mixing phase, the last element in the final buffer forms the resulting hash output that is sent to the normal sensed node. This is mathematically formulated as given below.

$$HV = H_m[B_m] \quad (14)$$

Finally, the decryption process is carried out in the destination sensed node to obtain original data, therefore preventing illegal access. The pseudo representation of Balloon Cryptographic Matyas–Meyer–Oseas Block compression-based Secure Routing in CRN is provided below.

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Input:</b> Primary Users ' $PU = PU_1, PU_2, \dots, PU_m$ ', Secondary Users ' $SU = SU_1, SU_2, \dots, SU_n$                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Output:</b> robust and secure data routing                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Step 1: <b>Initialization</b> ' $m$ ', ' $n$ '<br>Step 2: <b>Initialize</b> normal nodes ' $NN$ ', data packets ' $DP$ '<br>Step 3: <b>Begin</b><br>Step 4: <b>For</b> each Primary Users ' $PU$ ', Secondary Users ' $SU$ ', normal nodes ' $NN$ ' and data packets ' $DP$ '<br>//Generate Matyas–Meyer–Oseas Compression function results according to (11)<br>//Encryption<br>//Expansion<br>Step 5: Generate input vector results according to (12)<br>//Mixing<br>Step 6: Generate mixed results repeatedly for a specified number of iteration according to (13)<br>//Output<br>Step 7: Obtain last element from the mixing function resulting hash output<br>Step 9: Return hashed value to the normal sensed nodes ' $HV$ '<br>Step 9: <b>End for</b><br>Step 11: <b>For</b> each Primary Users ' $PU$ ', Secondary Users ' $SU$ ', normal nodes ' $NN$ ' and data packets ' $DP$ '<br>Step 12: If ' $AHV = PHV$ '<br>Step 13: Then secured data routing between nodes<br>Step 14: End if<br>Step 15: <b>If</b> ' $AHV \neq PHV$ '<br>Step 16: <b>Then</b> no data routing between nodes<br>Step 17: <b>End if</b><br>Step 18: <b>End for</b><br>Step 19: <b>End</b> |

Algorithm 2 Balloon Cryptographic Matyas–Meyer–Oseas Block compression-based Secure Routing.  
Source: Authors, (2026).

As given in the above algorithm the entire process of blockchain-based secure data routing in cRN by combining the Balloon cryptographic hash with the Matyas–Meyer–Oseas compression function.

On one hand, Balloon Hashing necessitates a fundamental standard compression function and on the other hand, the Matyas-Meyer-Oseas compression function that is built from block cipher that serves this purpose. Balloon Hashing using Matyas-Meyer-Oseas compression function processes the input data to generate unique hash value that is sent to the sender node. On the other end the receiver node evaluates the hash and making a comparison with original hash as send by the server, any data packet changes results in a distinct hash value. In this manner the data integrity is ensured. Moreover by storing and distributing hashed data instead of the raw data packets using Matyas-Meyer-Oseas compression function in a blockchain helps prevent unauthorized data access wherein even if an unauthorized user intercepts hash value, original data packet is not reconstructed from hash. This in turn ensures data confidentiality.

### III.3 CASE STUDY AND INFERENCES

In this section case analysis of secure routing in CRN using primary and secondary users are simulated by applying eXtreme Gradient Boost Quadratic Balloon Cryptographic Block Compression (XGBQ-BCBC) method. Figure 4 shows the sample nodes for simulation.

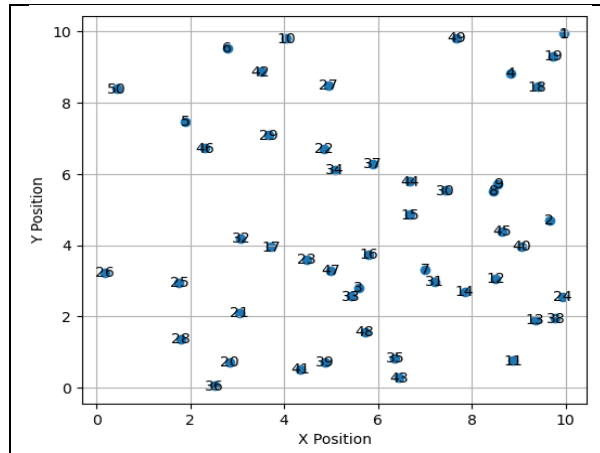


Figure 4: Sample node generation.

Source: Authors, (2026).

As shown in the above figure 50 nodes comprising of both primary user and secondary user are obtained for performing secure routing in CRN. To perform simulation 33 numbers of primary user and 17 numbers of secondary users are used. Also an initial energy of 100 Joules is set for all the 50 nodes and according to the proceedings the energy consumption gets depleted. With this hypothesis residual energy and relative trustworthiness factors are analyzed. The results are shown in figure 5.

| node_id | residual_energy | trust_value | user_type |    |
|---------|-----------------|-------------|-----------|----|
| 0       | 1               | 98.500000   | 0.976700  | PU |
| 1       | 2               | 97.000000   | 0.968400  | PU |
| 2       | 3               | 95.500000   | 0.960100  | PU |
| 3       | 4               | 94.000000   | 0.951800  | PU |
| 4       | 5               | 92.500000   | 0.943500  | PU |
| 5       | 6               | 91.000000   | 0.935200  | PU |
| 6       | 7               | 89.500000   | 0.926900  | PU |
| 7       | 8               | 88.000000   | 0.918600  | PU |
| 8       | 9               | 86.500000   | 0.910300  | PU |
| 9       | 10              | 85.000000   | 0.902000  | PU |
| 10      | 11              | 83.500000   | 0.893700  | PU |
| 11      | 12              | 82.000000   | 0.885400  | PU |
| 12      | 13              | 80.500000   | 0.877100  | PU |
| 13      | 14              | 79.000000   | 0.868800  | PU |
| 14      | 15              | 77.500000   | 0.860500  | PU |
| 15      | 16              | 76.000000   | 0.852200  | PU |
| 16      | 17              | 74.500000   | 0.843900  | PU |
| 17      | 18              | 73.000000   | 0.835600  | PU |
| 18      | 19              | 71.500000   | 0.827300  | PU |
| 19      | 20              | 70.000000   | 0.819000  | PU |
| 20      | 21              | 68.500000   | 0.810700  | PU |
| 21      | 22              | 67.000000   | 0.802400  | PU |
| 22      | 23              | 65.500000   | 0.794100  | PU |
| 23      | 24              | 64.000000   | 0.785800  | PU |
| 24      | 25              | 62.500000   | 0.777500  | PU |
| 25      | 26              | 61.000000   | 0.769200  | PU |
| 26      | 27              | 59.500000   | 0.760900  | PU |
| 27      | 28              | 58.000000   | 0.752600  | PU |
| 28      | 29              | 56.500000   | 0.744300  | PU |
| 29      | 30              | 55.000000   | 0.736000  | PU |
| 30      | 31              | 53.500000   | 0.727700  | PU |
| 31      | 32              | 52.000000   | 0.719400  | PU |
| 32      | 33              | 50.500000   | 0.711100  | PU |
| 33      | 34              | 49.000000   | 0.702800  | SU |
| 34      | 35              | 47.500000   | 0.694500  | SU |
| 35      | 36              | 46.000000   | 0.686200  | SU |
| 36      | 37              | 44.500000   | 0.677900  | SU |
| 37      | 38              | 43.000000   | 0.669600  | SU |
| 38      | 39              | 41.500000   | 0.661300  | SU |
| 39      | 40              | 40.000000   | 0.653000  | SU |
| 40      | 41              | 38.500000   | 0.644700  | SU |
| 41      | 42              | 37.000000   | 0.636400  | SU |
| 42      | 43              | 35.500000   | 0.628100  | SU |
| 43      | 44              | 34.000000   | 0.619800  | SU |
| 44      | 45              | 32.500000   | 0.611500  | SU |
| 45      | 46              | 31.000000   | 0.603200  | SU |
| 46      | 47              | 29.500000   | 0.594900  | SU |
| 47      | 48              | 28.000000   | 0.586600  | SU |
| 48      | 49              | 26.500000   | 0.578300  | SU |
| 49      | 50              | 25.000000   | 0.570000  | SU |

Figure 5: Calculation of residual energy and relative trustworthiness.

Source: Authors, (2026).

From the above results of residual energy and relative trustworthiness for each user in CRN, eXtreme Gradient Boost Node Classifier along with Quadratic classifier is applied to differentiate between normal nodes and malicious node. By differentiating between normal and malicious users, the authentication accuracy along with end-to-end delay involved in routing process gets improved. Figure 6 shows the corresponding results of normal primary user (33) and malicious users (i.e. secondary malicious users 14 and secondary normal users 13).

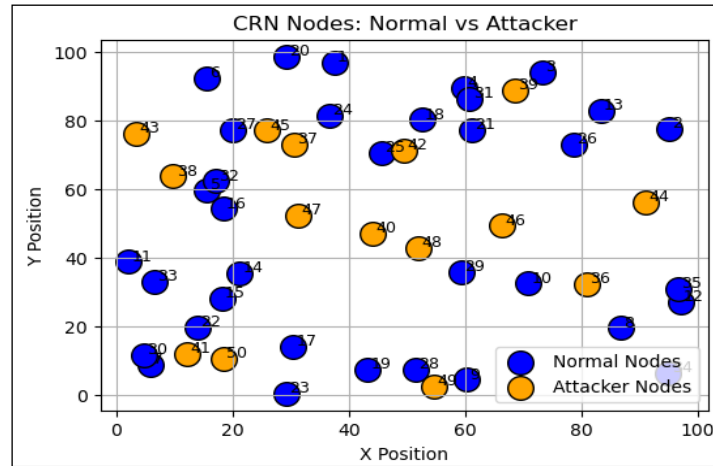


Figure 6: CRN Node Created Results  
Source: Authors, (2026).

Finally with the above CRN node created results, normal sensed data packets (i.e. with seven primary users and three secondary users for simulation) are subjected to Balloon Cryptographic hash-based Matyas–Meyer–Oseas compression to ensure secure routing. Figure 7 shows the cryptographic results generated to ensure authentication and integrity of data.

| node_id                                                                                                                                   | residual_energy | timestamp | trust_value       | block_hash | Cryptographic_hash(key)          | Cryptographic_hash(key)                   |
|-------------------------------------------------------------------------------------------------------------------------------------------|-----------------|-----------|-------------------|------------|----------------------------------|-------------------------------------------|
| 0                                                                                                                                         | 1               | 98.500000 | 1764305708.124430 | 0.976700   | 257403da1918b2b01a3c24ddcfad35c6 | 7e3299c816f7f0b56a7cc6703b2bd6b9          |
| 1                                                                                                                                         | 2               | 97.000000 | 1764305708.124697 | 0.968400   | cfdc435dcf216f5a81f4658b4bac1e4c | 866935708010f21815f1c7cce4e6af64          |
| 2                                                                                                                                         | 3               | 95.500000 | 1764305708.124897 | 0.960100   | e1c793b0c509fb71b010efc245eebcea | 1432345963ab2b2251e579b77dbaa67f          |
| 3                                                                                                                                         | 4               | 94.000000 | 1764305708.125081 | 0.951800   | 915ad44a24f7eb97534bcd165d1ba6cf | 9e419146f64f180dd1d6659db1020c80          |
| 4                                                                                                                                         | 5               | 92.500000 | 1764305708.125242 | 0.943500   | a2bdf0b248cda2f40b9462a513ec6a3a | 5b53f8e2b7bcb578a4ba39349dd94260          |
| 5                                                                                                                                         | 6               | 91.000000 | 1764305708.126130 | 0.935200   | be62c925840a79927647c7a2295e76d5 | 9d23eb7268c7151359b316731a86a279          |
| 6                                                                                                                                         | 7               | 89.500000 | 1764305708.126479 | 0.926900   | 6cb8a22a16cd5998d2c35d788653f7be | 99aa2522bd6f255d8ead70eb00f79aea          |
| 7                                                                                                                                         | 34              | 49.000000 | 1764305708.131452 | 0.702800   | 79746323359bd2b7302cb208330724cc | f183691e9126b2408f77ef81913ed26c          |
| 8                                                                                                                                         | 35              | 47.500000 | 1764305708.131587 | 0.694500   | 0dcf00bf0052ded5398159459a3c12e2 | 64e67c07b21557d5ec501bf90fb702a8          |
| 9                                                                                                                                         | 36              | 46.000000 | 1764305708.131728 | 0.686200   | 1ca9429c41e386a2ecd5a02b7e80fa5a | 27db2be29d7c29407af8e41a303d99b4          |
| Encoding results                                                                                                                          |                 |           |                   |            |                                  |                                           |
|                                                                                                                                           |                 |           |                   |            |                                  | decrypted_result    secure_routing_status |
| {"block_hash":"257403da1918b2b01a3c24ddcfad35c6","node_id":1,"residual_energy":98.5,"timestamp":1764305708.1244302,"trust_value":0.9767}  |                 |           |                   |            |                                  | Secured routing                           |
| {"block_hash":"cfdc435dcf216f5a81f4658b4bac1e4c","node_id":2,"residual_energy":97.0,"timestamp":1764305708.124697,"trust_value":0.9684}   |                 |           |                   |            |                                  | Secured routing                           |
| {"block_hash":"e1c793b0c509fb71b010efc245eebcea","node_id":3,"residual_energy":95.5,"timestamp":1764305708.1248972,"trust_value":0.9601}  |                 |           |                   |            |                                  | Secured routing                           |
| {"block_hash":"915ad44a24f7eb97534bcd165d1ba6cf","node_id":4,"residual_energy":94.0,"timestamp":1764305708.1250808,"trust_value":0.9518}  |                 |           |                   |            |                                  | Secured routing                           |
| {"block_hash":"a2bdf0b248cda2f40b9462a513ec6a3a","node_id":5,"residual_energy":92.5,"timestamp":1764305708.1252425,"trust_value":0.9435}  |                 |           |                   |            |                                  | Secured routing                           |
| {"block_hash":"be62c925840a79927647c7a2295e76d5","node_id":6,"residual_energy":91.0,"timestamp":1764305708.1261303,"trust_value":0.9352}  |                 |           |                   |            |                                  | Secured routing                           |
| {"block_hash":"6cb8a22a16cd5998d2c35d788653f7be","node_id":7,"residual_energy":89.5,"timestamp":1764305708.126479,"trust_value":0.9269}   |                 |           |                   |            |                                  | Secured routing                           |
| {"block_hash":"79746323359bd2b7302cb208330724cc","node_id":34,"residual_energy":49.0,"timestamp":1764305708.131452,"trust_value":0.7028}  |                 |           |                   |            |                                  | Secured routing                           |
| {"block_hash":"0dcf00bf0052ded5398159459a3c12e2","node_id":35,"residual_energy":47.5,"timestamp":1764305708.1315866,"trust_value":0.6945} |                 |           |                   |            |                                  | Secured routing                           |
| {"block_hash":"1ca9429c41e386a2ecd5a02b7e80fa5a","node_id":36,"residual_energy":46.0,"timestamp":1764305708.1317277,"trust_value":0.6862} |                 |           |                   |            |                                  | Secured routing                           |
| Decoded results for secure routing                                                                                                        |                 |           |                   |            |                                  |                                           |

Figure 7: Cryptographic results for secure routing.  
Source: Authors, (2026).

By applying the above Balloon Hashing using Matyas-Meyer-Oseas compression function unique hash values are generated that in turn results in the improvement of data integrity. Also by storing and distributing hashed data instead of the raw data packets improves the overall data confidentiality extensively. The quantitative results are provided in the following sub-section.

#### IV. EXPERIMENTAL SETUP

In this section, the performance of the proposed blockchain method called, eXtreme Gradient Boost Quadratic Balloon Cryptographic Block Compression (XGBQ-BCBC) based secured routing in CRN was analyzed. The proposed method was implemented using Python high-level general-purpose programming language and the experiments are performed on an Intel(R) Pentium machine with a speed 2.13 GHz and 4.0 GB RAM using Windows 7 32-bit Operating System. A brief comparison of the proposed XGBQ-BCBC method with the existing Channel Availability Probability [1] and Multi-objective optimization [2] with respect to authentication accuracy, authentication time, data confidentiality and data integrity for varied numbers of data packets and sensor nodes.

#### V. RESULTS AND DISCUSSION

The performance of the proposed XGBQ-BCBC and two existing approaches namely Channel Availability Probability [1] and Multi-objective optimization [2] are discussed. To evaluate the model's effectiveness, several performance indicators are considered, including authentication accuracy, authentication time, data confidentiality and data integrity.

##### V.1 PERFORMANCE ANALYSIS OF AUTHENTICATION ACCURACY

In this section authentication accuracy is analyzed and validated. Authentication and secure routing are said to be demanding as far as cognitive radio networks (CRNs) are concerned. This is due to the reason to make certain accurate spectrum sharing is made by verifying and validating node identities and establishing reliable data paths that is said to be demanding owing to the network's arbitrary nature. The authentication accuracy is mathematically stated as given below.

$$AA = \sum_{i=1}^N \frac{DP_{AA}}{DP_i} * 100 \quad (15)$$

From the above equation (15) authentication accuracy 'AA' is measured based on the data packets considered ' $DP_i$ ' and data packets authenticated accurately ' $DP_{AA}$ '. It is measured in terms of percentage (%). Table 1 lists the authentication accuracy results when substituted in equation (15).

Table 1: Authentication accuracy using Proposed XGBQ-BCBC, Existing Channel Availability Probability [1] and Multi-objective optimization.

| Number of users | Authentication accuracy (%) |                                      |                                  |
|-----------------|-----------------------------|--------------------------------------|----------------------------------|
|                 | Proposed XGBQ-BCBC          | Channel Availability Probability [1] | Multi-objective optimization [2] |
| 5               | 90                          | 85                                   | 80                               |
| 10              | 85.35                       | 76.25                                | 63.35                            |
| 15              | 84                          | 75.55                                | 62.45                            |
| 20              | 83.15                       | 74.25                                | 61.25                            |
| 25              | 82                          | 73                                   | 60                               |
| 30              | 80.45                       | 71.45                                | 58.15                            |
| 35              | 83.55                       | 74.35                                | 61.55                            |
| 40              | 85                          | 76                                   | 63.25                            |
| 45              | 87.15                       | 78.15                                | 65.15                            |
| 50              | 89                          | 80                                   | 67                               |

Source: [2].

Table 1 demonstrates the experimental results of authentication accuracy. The number of users is taken in the ranges from 5 to 50. Table 1 symbolizes the performance evaluation of the authentication accuracy using three techniques proposed XGBQ-BCBC and existing methods Channel Availability Probability [1] and Multi-objective optimization [2]. Let us consider the 5 user for conducting the experiments. Firstly, the authentication accuracy is obtained as 90%, 85% and 80% for proposed XGBQ-BCBC and existing [1], [2] respectively. Similarly, nine remaining runs are carried out with respect to the number of users. The observed ten results of the XGBQ-BCBC are compared to the existing methods. The graph is created as given below figure 8 based on the above table 1.

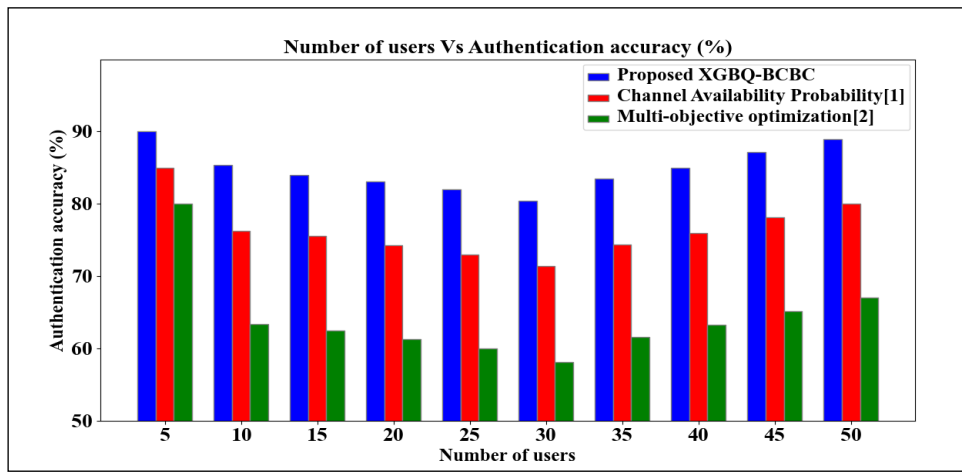


Figure 8: Analysis of authentication accuracy.

Source: Authors, (2026).

Figure 8 shows the results of authentication accuracy using three methods, XGBQ-BCBC, Channel Availability Probability [1] and Multi-objective optimization [2]. To ensure fair comparison between three methods, similar number of users (PUs and SUs) ranging between 5 and 50 are applied to simulation process. The horizontal axis denotes the number of users, while the vertical axis reflects the authentication accuracy achieved. An increase in number of users causes increase in the spectrum utilization by the secondary user in case of channel availability and hence in the presence of malicious secondary user accuracy is said to be compromised. However simulations conducted for 10 iterations show high authentication accuracy results generated for the proposed XGBQ-BCBC method upon comparison to [1] and [2]. The reason for higher authentication accuracy is to apply the eXtreme Gradient Boost Node Classifier. It combines the weak classifier result for achieving the strong classifier output. Quadratic Classifier is considered as weak classifier to accurately classify the nodes as normal nodes or malicious nodes. With this the overall authentication accuracy using proposed XGBQ-BCBC method was found to be better by 10% compared to [1] and 33% compared to [2].

## V.2 PERFORMANCE ANALYSIS OF END-TO-END DELAY

End-to-end delay in secure routing for cognitive radio networks is a performance metric denoting the total time consumed for a data packet to travel between source and destination. This is mathematically formulated as given below.

$$E2E6 = T_{i\text{ End}} - T_{i\text{ Start}} \quad (16)$$

From the above equation (16) end-to-end delay 'E2E' denotes the time consumed ' $T_{i\text{ End}}, T_{i\text{ Start}}$ ' between the source and destination to transmit data packets between them. It is measured in terms of seconds (sec). Table 2 lists the end-to-end delay results when substituted in equation (16).

Table 2: End-to-end delay using Proposed XGBQ-BCBC, Existing Channel Availability Probability and Multi-objective optimization.

| Number of users | End-to-end delay (sec) |                                      |                                  |
|-----------------|------------------------|--------------------------------------|----------------------------------|
|                 | Proposed XGBQ-BCBC     | Channel Availability Probability [1] | Multi-objective optimization [2] |
| 5               | 4.4                    | 5.25                                 | 7.55                             |
| 10              | 6.3                    | 8.25                                 | 8.85                             |
| 15              | 7.1                    | 10.45                                | 10.95                            |
| 20              | 10.45                  | 12.95                                | 13.25                            |
| 25              | 12.1                   | 14.45                                | 14.85                            |
| 30              | 13.25                  | 15.35                                | 15.85                            |
| 35              | 12.45                  | 14.65                                | 16                               |
| 40              | 10.1                   | 12.25                                | 14.15                            |
| 45              | 9.25                   | 10.45                                | 11.35                            |
| 50              | 11.1                   | 13.1                                 | 13.55                            |

Source: [1] [2].

Table 2 demonstrates the performance analysis outcomes of end-to-end delay. The results of end-to-end delay using XGBQ-BCBC with existing Channel Availability Probability [1] and Multi-objective optimization [2]. But, comparatively, proposed XGBQ-BCBC minimizes the end-to-end delay involved during the secure routing. With the increasing number users, results of end-to-end delay are increased. By considering the values in above table 2, the graph is plotted in figure 9.

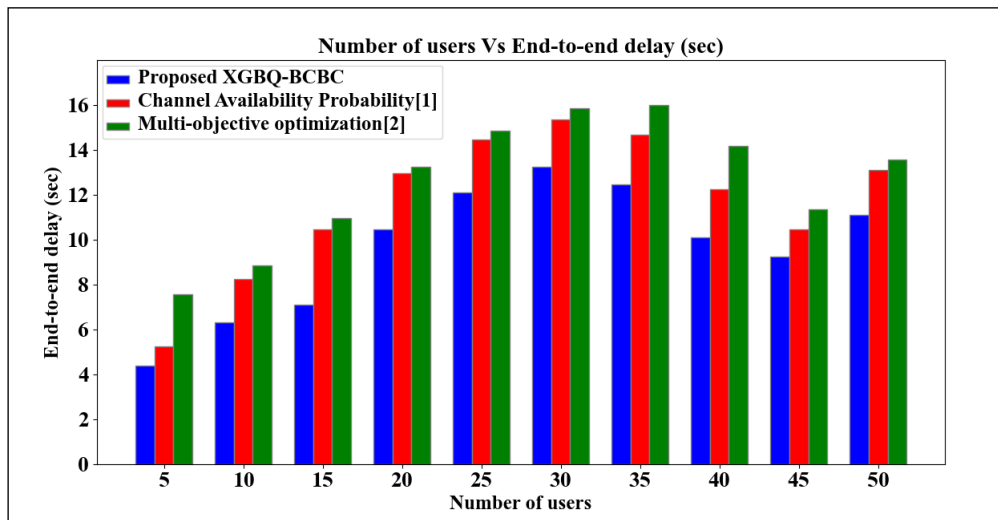


Figure 9: Analysis of end-to-end delay.

Source: Authors, (2026).

Figure 9 shows the graphical representation of end-to-end delay recorded for three distinct methods, XGBQ-BCBC, Channel Availability Probability [1] and Multi-objective optimization [2] respectively. Values were substituted in equation (16) and results were plotted accordingly for all the three methods. Though an increase in the end-to-end delay is recorded for the first six iterations however for rest of the four iterations the end-to-end delay was found to be decreasing, therefore corroborating the objective of increase in number of users does not influence end-to-end delay. However, the 10 users are considered for calculating the end-to-end delay. Firstly, the end-to-end delay is obtained as 6.3sec using proposed XGBQ-BCBC method. By applying the [1] [2], the end-to-end delay is found to be 8.25sec and 8.85sec respectively. Also simulations performed for an overall ten simulation runs show comparatively better results using proposed XGBQ-BCBC method than [1] and [2]. The reason was by applying the eXtreme Gradient Boost Quadratic Node Classifier where classification of nodes between normal and malicious was performed. Also, the residual energy is measured. The nodes are chosen with high residual energy for routing. Node trustworthiness is evaluated using a likelihood ratio. The combination of these techniques is intended to reduce the end-to-end delay. This in turn minimized the end-to-end delay involved in the process of routing in CRN using XGBQ-BCBC method by 23% compared to [1] and 35% compared to [2] respectively.

### V.3 PERFORMANCE ANALYSIS OF DATA CONFIDENTIALITY

In this section data confidentiality rate is analyzed. Data confidentiality prevents unauthorized access to data packets making certain that only authorized cognitive users view it. In this manner sensitive data packet information are protected from unauthorized access. The data confidentiality is represented as given below.

$$DC = \sum_{i=1}^N \frac{DP_{ACU}}{DP_i} * 100 \quad (17)$$

From the above equation (17) data confidentiality ‘DC’ is measured based on the data packets considered ‘ $DP_i$ ’ and the data packets accessed by authenticated cognitive users ‘ $DP_{ACU}$ ’. Table 3 lists the data confidentiality rate results when substituted in equation (17).

Table 3: Data confidentiality using Proposed XGBQ-BCBC, Existing Channel Availability Probability and multi-objective optimization.

| Data packets | Data confidentiality (%) |                                      |                                  |
|--------------|--------------------------|--------------------------------------|----------------------------------|
|              | Proposed XGBQ-BCBC       | Channel Availability Probability [1] | Multi-objective optimization [2] |
| 50           | 98                       | 90                                   | 84                               |
| 100          | 96.26                    | 86.54                                | 81.25                            |
| 150          | 94                       | 84.35                                | 79.35                            |
| 200          | 93.15                    | 83.15                                | 78.55                            |
| 250          | 92                       | 82.55                                | 77.65                            |
| 300          | 90.55                    | 80.15                                | 75.35                            |
| 350          | 88.65                    | 78.35                                | 73.25                            |
| 400          | 90                       | 80.25                                | 75.55                            |
| 450          | 93.15                    | 83.55                                | 78.15                            |
| 500          | 95                       | 85                                   | 75                               |

Source: [1] [2].

Table 3 describes the performance results of data confidentiality rate versus the data packets considered in the ranges from 50 to 500. The performance of data confidentiality rate is computed using three methods namely proposed XGBQ-BCBC method and existing methods, Channel Availability Probability [1] and Multi-objective optimization [2]. The overall observed results indicate that the XGBQ-BCBC method provides improved performance in terms of achieving higher data confidentiality (i.e., higher data transmission) than the existing methods. This is proved through the statistical calculation. For considering 50 data packets, the data confidentiality is significantly improved using the proposed effectively increased using the XGBQ-BCBC by 98% when compared to existing methods taken for comparison Channel Availability Probability [1] (90%), Multi-objective optimization [2] (84%). The graph is plotted as given below figure 10 based on the above table 3.

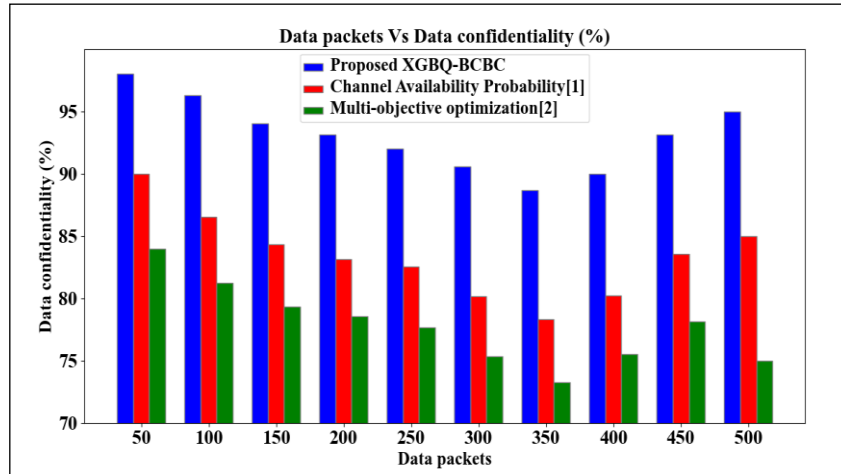


Figure 10: Analysis of Data Confidentiality.  
Source: Authors, (2026).

Figure 10 shows the results of data confidentiality for the proposed XGBQ-BCBC method and two existing methods, Channel Availability Probability [1] and Multi-objective optimization [2] respectively. From the above figure data confidentiality was observed to be lesser for the first set of seven iterations whereas for the rest of three iterations it was found to be higher. Also comparative figurative representation show better results using proposed XGBQ-BCBC method when compared to [1] and [2]. The reason was by applying Balloon Cryptographic hash function for secured data routing and Matyas–Meyer–Oseas (MMO) compression function for hash generation in a blockchain control plane. Hash value is converted into original data with fixed-size. MMO process is one-way function to reverse the hash to find the original raw data. Storing and distributing only the hashed data in the blockchain control plane that enhances data confidentiality. An unauthorized party who accesses the hash value cannot view the original content. This in turn improves data confidentiality of the proposed XGBQ-BCBC method by 10% compared to [1] and 16% compared to [2].

#### V.4 PERFORMANCE ANALYSIS OF DATA INTEGRITY

In this section data integrity analysis is made. Data integrity ensures that data packets are accurate and have not been tampered with or changed in an unauthorized manner. With this unauthorized or accidental modification of data is said to be avoided. The data integrity rate is mathematically formulated as given below.

$$DI = \sum_{i=1}^N \frac{DP_{NM}}{DP_i} * 100 \quad (18)$$

From the above equation (18) data integrity 'DI' is measured based on the data packets considered 'DP<sub>i</sub>' and the amount of data packets being not modified 'DP<sub>NM</sub>'. Table 4 lists the data integrity rate results when substituted in equation (18).

Table 4: Data integrity using Proposed XGBQ-BCBC, Existing Channel Availability Probability and multi-objective optimization.

| Data packets | Data integrity (%) |                                      |                                  |
|--------------|--------------------|--------------------------------------|----------------------------------|
|              | Proposed XGBQ-BCBC | Channel Availability Probability [1] | Multi-objective optimization [2] |
| 50           | 94                 | 88                                   | 82                               |
| 100          | 91.35              | 79.35                                | 74.25                            |
| 150          | 90.25              | 78.55                                | 73.15                            |
| 200          | 88.55              | 76.35                                | 71.55                            |
| 250          | 85.35              | 73.25                                | 68.25                            |
| 300          | 82                 | 70.1                                 | 65.55                            |
| 350          | 80                 | 68.45                                | 63.25                            |
| 400          | 84.15              | 72.15                                | 67.55                            |
| 450          | 87                 | 75.35                                | 70.25                            |
| 500          | 89.25              | 77.35                                | 72.15                            |

Source: [1] [2].

Table 4 demonstrates the performance analysis outcomes of data integrity rate. The data packets are considered in the range from 50 to 500. The validation is performed through comparing proposed XGBQ-BCBC method and two existing methods, Channel Availability Probability [1] and Multi-objective optimization [2]. With the increasing number of data packets, results of data integrity rate are reduced or increased. However, the proposed XGBQ-BCBC method is achieved better data integrity rate than the other two conventional methods.

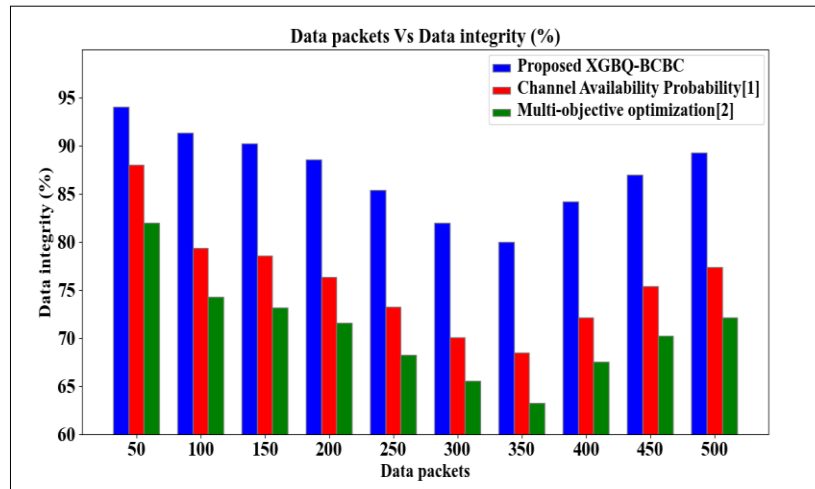


Figure 11: Analysis of data integrity.

Source: Authors, (2026).

Finally figure 11 give above illustrates the data integrity results using three methods, XGBQ-BCBC, Channel Availability Probability [1] and multi-objective optimization [2]. With horizontal axis representing the data packets ranging between 50 and 500, vertical axis denotes the data integrity results by applying the values in the equation 18. This is evident from the simulation with 50 data packets where the data integrity using XGBQ-BCBC was observed to be 94% whereas the data integrity for [1] and [2] was found to be 88% and 82% respectively. Comparison between three methods shows better data integrity results for XGBQ-BCBC method when compared to [1] and [2]. The reason for higher data integrity was to employ the Balloon Hashing using Matyas-Meyer-Oseas compression function. By using this algorithm, unique hash value are generated for each input data that is sent to the sender node. Evaluates the hash of the received data and compares it to the original hash value sent by the sender. A successful comparison confirms that the data has not been altered during transmission, therefore ensuring the data integrity and enabling routing. With this the data integrity of XGBQ-BCBC method was found to be better by 13% compared to [1] and 19% compared to [2].

## VI. CONCLUSION

This paper presented a novel blockchain method to ensure secured routing in cognitive radio network using eXtreme Gradient Boost Quadratic Balloon Cryptographic Block Compression (XGBQ-BCBC) method. The proposed XGBQ-BCBC method for secure routing in CRN performed via blockchain performs the tasks of user (PU and SU) registration, block generation, node classification between normal users, malicious users and establishing data routing between normal nodes. First, user registration process was performed and stored in the form of blocks via blockchain. Following which for each registered user, eXtreme Gradient Boost Quadratic Node Classifier was applied differentiating between normal users and malicious users based on the likelihood ratio via residual energy and relative trustworthiness factors. Finally, with the data packets of sensed normal users using Balloon Cryptographic Matyas-Meyer-Oseas (MMO) Block compression results secure routing is established in an accurate manner. The algorithm is designed to simultaneously optimize four distinct performance metrics, including authentication accuracy, end-to-end delay, data confidentiality and data integrity. The proposed XGBQ-BCBC is assessed on various numbers of data packets and users. The performance of the proposed method is compared to the popular secure routing methods such as Channel Availability Probability and multi-objective optimization using different performance metrics. Experimental results prove that the XGBQ-BCBC method efficiently differentiates between normal and malicious users and therefore ensuring secure routing.

## VII. AUTHOR'S CONTRIBUTION

**Conceptualization:** T. Sundar, A. Senthilkumar.

**Methodology:** T. Sundar, A. Senthilkumar.

**Investigation:** T. Sundar, A. Senthilkumar.

**Discussion of results:** T. Sundar, A. Senthilkumar.

**Writing – Original Draft:** T. Sundar, A. Senthilkumar.

**Writing – Review and Editing:** T. Sundar, A. Senthilkumar.

**Resources:** T. Sundar, A. Senthilkumar.

**Supervision:** T. Sundar, A. Senthilkumar.

**Approval of the final text:** T. Sundar, A. Senthilkumar.

## VIII. REFERENCES

- [1] Qusay M. Salih, Md Arafatur Rahman, A. Taufiq Asyhari, Muhammad Kamran Naeem, Mohammad Patwary, Ryan Alturki and Mohammed Abdulaziz Ikram, "Dynamic channel estimation-aware routing protocol in mobile cognitive radio networks for smart IIoT applications", *Digital Communications and Networks*, Elsevier, Volume 9, Issue 2, April 2023, Pages 367-382 [Channel Availability Probability].
- [2] Zhongguo Zhou, You Li, Ziming Zhu, Qinghe Gao, Sisi Xiao, Tao Yan and Yan Huo, "A cognitive spectrum allocation scheme for data transmission in smart distribution grids", *High-Confidence Computing*, Volume 4, 2024, Pages 1-9 [multi-objective optimization].
- [3] Evelyn Ezhilarasi I and J. Christopher Clement, "Robust Cooperative spectrum sensing in Cognitive Radio Blockchain network using SHA-3 algorithm", *Blockchain: Research and Applications*, Elsevier, 2024, Pages 1-18.
- [4] Archit Jain, Nitin Gupta and M. Sreenu, "Blockchain based smart contract for cooperative spectrum sensing in cognitive radio networks for sustainable beyond 5G wireless communication", *Green Technologies and Sustainability*, Elsevier, Volume 1, Issue 2, May 2023, Pages 1-10.
- [5] D. Balakumar, S. Nandakumar, "Blockchain-enabled cooperative spectrum sensing in 5G and B5G cognitive radio via massive multiple-input multiple-output nonorthogonal multiple access", *Results in Engineering*, Elsevier, Vol. 24, Dec 2024.
- [6] Hamad Aldawsari, "A blockchain-based approach for secure energy-efficient IoT-based Wireless Sensor Networks for smart cities", *Alexandria Engineering Journal*, Elsevier, Vol. 126, Jul 2025.
- [7] S. Ramachandra, M. Baskar, "Real-time multi-level trust-based secure routing for improved QoS in WSN using blockchain", *Results in Engineering*, Elsevier, Vol. 26, Jun 2025.
- [8] Nikhil Kumar Marriwala, Sunita Panda, Chandran Kamalanathan, Narayanan Sadhasivam, Vootla Subba Ramaiah, "An Analytical Model for Dynamic Spectrum Sensing in Cognitive Radio Networks Using Blockchain Management", *Engineering Proceedings*, MDPI, Mar 2023.
- [9] Sidra Tul Muntaha Pavlos, I. Lazaridis, Maryam Hafeez, Qasim Z. Ahmed, Zaharias D. Zaharis, Faheem A. Khan, "Blockchain for Dynamic Spectrum Access and Network Slicing: A Review", *IEEE Access*, Vol. 11, Feb 2023.
- [10] Nassmah Y. Al-Matari, Ammar T. Zahary, Asma A. Al-Shargabi, "A survey on advancements in blockchain-enabled spectrum access security for 6G cognitive radio IoT networks", *Scientific Reports*, Nov 2024.
- [11] Mai Shawkat, Ali El desoky, Zainab H. Ali, Mofreh Salem, "Blockchain and federated learning based on aggregation techniques for industrial IoT: A contemporary survey", *Peer-to-Peer Networking and Applications*, Springer Nature Link, Vol. 18, May 2025.
- [12] Senthil Kumar Jagatheesaperumal Abdellah Chehri, Mohamed Rahouti, Kaiqi Xiong, Janbueniek, "Blockchain-Based Security Architecture for Uncrewed Aerial Systems in B5G/6G Services and Beyond: A Comprehensive Approach", *IEEE Open Journal of the Communications Society*, Vol. 6, Jan 2025.
- [13] Abir Raza, Elarbi Badidi, Omarel Harrouss, Mohammad Hayajneh, Ezedin Barka, "Blockchain-Based Reputation and Trust Management for Smart Grids, Healthcare, and Transportation: A Review", *IEEE Access*, Vol. 12, Dec 2024.
- [14] Sidra Tul Muntaha Pavlos, Maryam Hafeez, Qasim Z. Ahmed, Zaharias D. Zaharis, Faheem A. Khan, "Blockchain for Dynamic Spectrum Access and Network Slicing: A Review", *IEEE Access*, Vol. 11, Feb 2023.
- [15] Khan Maaz Bin Hasan Ketan Kotecha, Mohammad Sajid, Maria A. Lapina, Mohammad Shahid, "Blockchain technology meets 6 G wireless networks: A systematic survey", *Alexandria Engineering Journal*, Elsevier, Vol. 92, Apr 2024.
- [16] Debabrata Dansana, Prafulla Kumar Behera, S. Gopak Krishna Patro, Quadri Noorulhasan Naveed, Ayodele Lasisi, Anteneh Wogasso Wodajo, "BSMACRN: Design of an Efficient Blockchain Based Security Model for Improving Attack-Resilience of Cognitive Radio Ad-hoc Networks", *IEEE Access*, Vol. 12, Jan 2024.
- [17] Saraswathi Vedachalam, Dayanaraj, "Development of a Privacy-Preserved and Secure Cooperative Spectrum Sensing System in Cognitive Radio Networks Using ATSNRNN-Enabled FPPDES With Machine Learning", *IEEE Access*, Vol. 12, Nov 2024.
- [18] Sadia Hussain, Shahzaib Tahir, Hasan Tahir, Asif Masood, "Blockchain-Enabled Secure Communication Framework for Enhancing Trust and Access Control in the Internet of Vehicles (IoV)", *IEEE Access*, Vol. 12, Aug 2024.
- [19] Mohammed A Alghamdi, "An Optimized and Secure Energy-Efficient Blockchain-Based Framework in IoT", *IEEE Access*, Vol. 13, Dec 2022.
- [20] Debabrata Dansana, Prafulla Kumar Behera, Abdul Basit, A. Darem Zubair Ashraf, Abutahazamani, Mohammad Nadeem Ahmed, Gopal Krishna Patro, Mohammad Shameem, "BDDTPA: Blockchain-Driven Deep Traffic Pattern Analysis for Enhanced Security in Cognitive Radio Ad-Hoc Networks", *IEEE Access*, Vol. 11, Sep 2023.
- [21] D. Balakumar, Nandakumar Sendrayan, "Enhance the Probability of Detection of Cooperative Spectrum Sensing in Cognitive Radio Networks Using Blockchain Technology", *Journal of Electrical and Computer Engineering*, Hindawi, Dec 2023.
- [22] K. Saravanan, K. B. Gurumoorthy, Allwin Devaraj Stalin, Om Prakash Kumar, "Secure channel estimation model for cognitive radio network physical layer security using two level shared key authentication", *Scientific Reports*, Oct 2025.
- [23] Deepanramkumar Pari, Jaisankar Natarajan, "Secure Spectrum Access, Routing, and Hybrid Beamforming in an Edge-Enabled mmWave Massive MIMOCRN-Based Internet of Connected Vehicle (IoCV) Environments", *Sensors*, MDPI, Dec 2022.
- [24] Ankita Sharma, Shalli Rani, Wadii Boulila, "Blockchain-based zero trust networks with federated transfer learning for IoT security in industry 5.0", *PLOS One*, Jun 2025.
- [25] Haitham Mahmoud, Junai Darshad, Adelaneiba, "A Systematic Review of Blockchain-Based Privacy-Preserving Reputation Systems for IoT Applications", *Distributed Ledger Technologies: Research and Practice*, ACM, Vol. 3, Dec 2024.

- [26] Geetanjali Rathee, Ashutosh Sharma, Razi Iqbal, Moayad Aloqaily, Rajiv Kumar, Naveen Jaglan, “ABlockchain Framework for Securing Connected and Autonomous Vehicles”, Sensors, MDPI, Nov 2019.
- [27] Nitesh Ghodichor, Raj Thaneeghavl. V, Dinesh Sahu, Gautam Borkar, Ankush Sawarkar, “Secure Routing Protocol to Mitigate Attacks by using Blockchain Technology in MANET”, International Journal of Computer Networks & Communications, Vol. 15, Mar 2023.
- [28] K. R. Chairma Lakshmi, “Blockchain-Based Routing Protocols for Secure Data Transmissino”, ICTACT Journal on Communication Technology, Vol. 15, Sep 2024.
- [29] Jameel Ahmad, Muhammad Umer Zia, Ijaz Haider Naqvi, Jawwad Nasar Chattha, Faran Awais Butt, Tao Huang, Wei Xiang, “Machine learning and blockchain technologies for cyber security in connected vehicles”, Wiley, Aug 2023.
- [30] Hilmi Lazrag, Rachid Saadane, Moulay Dirss Rahmani, “ABlockchain-based Approach for Optimal and Secure Routing in Wireless Sensor Networks”, International Conference on Signal-image Technology and Internet Based Systems.