

Cognitive Trust-PQZTA: An AI-Driven Post-Quantum Zero-Trust Blockchain Framework for Secure and Adaptive Routing in Cognitive Radio Networks

T. Sundar¹, Dr. A. Senthilkumar²

¹Ph.D. - Research Scholar, Department of Computer Science, Periyar University, Salem, Tamil Nadu, India – 636011

²Assistant professor, Department of Computer Science, Thiruvalluvar Government Arts College, Affiliated to Periyar University, Rasipuram, Tamil Nadu, India – 637401

Abstract—A Cognitive Radio Networks (CRNs) uses the flexibility of the spectrum by dynamically accessing the available spectrum bands to achieve more efficient utilization of the spectrum. But with the dynamic topology and limited energy, malicious nodes, spectrum variability and emerging quantum threats come with serious challenges in communication security and reliability. Existing CRN routing and security strategies typically involve trust management, routing, authentication, or encryption, or blockchain alone, each with only partial adaptability and comprehensive protection. This research proposes an innovative framework of Cognitive Trust-PQZTA which is proposed for secure and adaptive routing in CRNs. For node trust, the proposed framework first uses the Temporal Federated Trust-Energy Reputation Network (TFTERN) to assess the trust of nodes according to the behavioral information, residual energy, packet-forwarding consistency, spectrum-access behavior, and historical reputation. Then Temporal Graph Attention Transformer (TGAT) is used to predict reliable candidate routes and learn the dynamic spatial-temporal relationship. The Adaptive Multi-Objective Manta Ray Optimization (AM-MRMO) technique optimizes the set of selected routes based on hop count, delay, energy consumption, routing overhead, exposure to malicious node, routing reliability, and spectrum stability. The Post-Quantum Adaptive ECC-Kyber Hybrid Encryption (PAEKHE) mechanism ensures secure establishment of a session-key and data protection. The Continuous Risk-Adaptive Zero-Trust Authentication (CRAZTA) mechanism continuously assesses the risk of an entity and deviations from its behavior. Lastly, Reputation-Aware Proof-of-Authority Byzantine Fault-Tolerant (RA-PoA-BFT) verifies transactions by using decentralized blockchain consensus, for authentication and routing.

The proposed framework is designed to enhance the reliability of the routing, security, energy efficiency, resistance to attacks, authentication accuracy, and computational efficiency.

Index Terms—Cognitive Radio Networks, Secure Routing, Trust Management, Zero-Trust Authentication, Blockchain, Post-Quantum Cryptography, Adaptive Routing, Trust Evaluation.

I. INTRODUCTION

Modern, communication technologies have made a significant progress and the need for secure, reliable and decentralized communication infrastructures has grown significantly. In emerging applications like smart grid, wireless communication systems, CRNs, and intelligent communication services, there is a need for secure data transmission with the assurance of confidentiality, integrity, authentication and trust. Centralized communication systems are susceptible to advanced cyber-attacks due to their inherent weaknesses in single points of failure, potential data tampering, unauthorized access and limited scalability. The technology of blockchain has proved to be a useful solution, offering distributed entities reliable communication and integrity, immutable transaction records, cryptographic security, and decentralized ledger management [1].

Blockchain technology securely shares communication transactions, verifies them using distributed consensus mechanisms, calculates cryptographic hash values and records valid transactions on an immutable distributed ledger. This

decentralized approach ensures data integrity, fosters transparency, and offers secure communication in today's network infrastructure. In smart grid applications, lightweight smart contract frameworks are proposed to decrease the computation burden and secure communication, and efficient transaction processing [2]. Likewise, blockchain based wireless communication systems enhance authentication, information sharing security and privacy protection in distributed communication systems [3].

The development of CRNs has become fast and the role of intelligent trust management and adaptive spectrum sharing has become more significant. Using blockchain-inspired trust management, decentralized trust management, cooperative spectrum sensing, and reliable node selection can be achieved to enhance the security of communications and spectrum utilization. Such mechanisms provide greater resistance to malicious nodes as well as trustworthy communication in dynamic wireless environment [4]. Artificial Intelligence (AI) has revolutionized communication networks, facilitating intelligent decision-making, automated threat detection, predictive analysis, and adaptive resource optimization. AI-powered methods use big communication data to spot abnormal network activity, enhance resource usage and boost

communication effectiveness. The combination of AI and blockchain technology further strengthens the adaptive security management, intelligent trust computation and autonomous communication control, which makes next generation communication networks more secure, scalable and reliable [5].

Although these developments have been made, there is still a lack of scalability in the current blockchain-based communication systems, communication delay, dynamic trust management, transaction latency, and computational overhead. Thus, by combining lightweight blockchain designs, intelligent trust management, and AI optimization of communications, one can effectively design a secure, efficient, scalable, and resilient next-generation communications network. Figure 1 shows the architecture of the proposed AI-Enabled Blockchain Based Secure Communication Framework, where the communication data is gathered from smart grid, wireless, and CRN devices followed by applying the AI techniques. This approach combines lightweight smart contracts with blockchain security, trust management, and secure data storage, ensuring reliable, decentralized, and secure communication services.

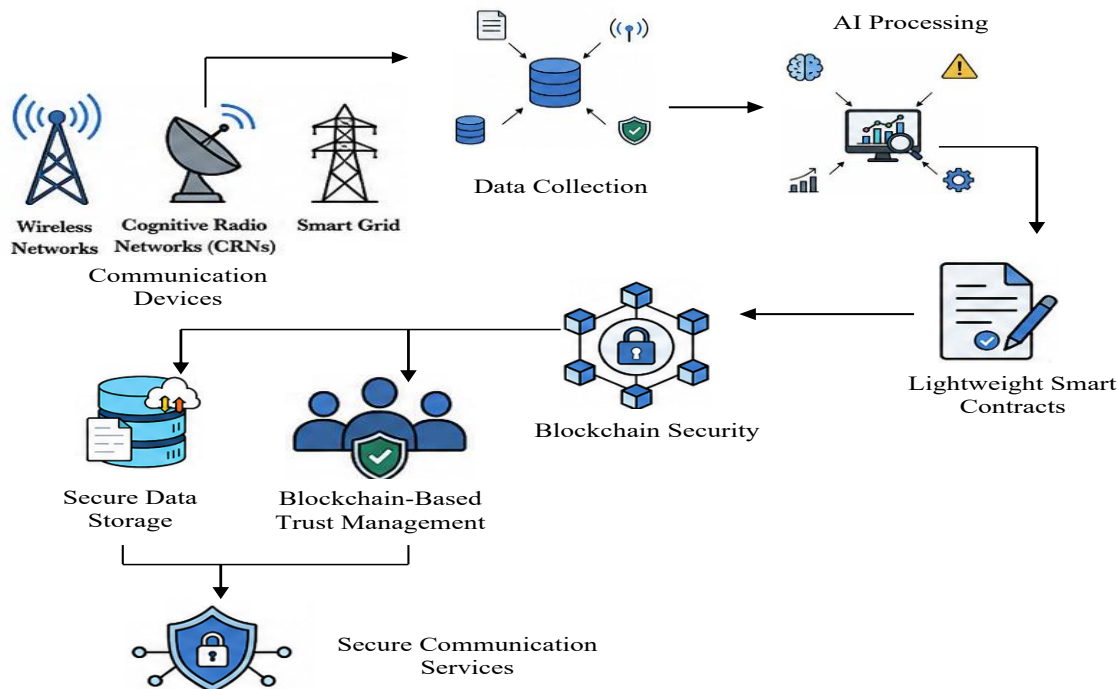


Figure 1. Architecture of AI-Enabled Blockchain-Based Secure Communication Framework

A. Contribution of the Work

- Presented a TFTERN mechanism to measure node's trust and reputation with the help of behavioural information, residual energy, packet-forwarding consistency, spectrum-access behaviour, and historical reputation.
- Proposed a TGAT model for learning the dynamic spatial-temporal relationship among CRN nodes and find reliable candidate routes.
- Proposed an AM-MRMO optimization technique that can select the optimal communication route based on the hop count, delay, energy cost, routing overhead, malicious-node exposure, path reliability, and spectrum stability.
- Designed a PAEKHE mechanism that integrates ECC and Kyber for a secure establishment of session-keys and protection of data against emerging quantum threats.
- Implements CRAZTA to continuously monitor the risk level of an entity and deviations from its behavior for adaptive zero-trust authentication in communication.
- Proposed RA-PoA-BFT to enable validation of authentication and routing transactions using a decentralized blockchain consensus that is reputation-aware Proof-of-Authority and Byzantine Fault-Tolerant.
- Designed the whole framework of CognitiveTrust-PQZTA that enhances the reliability of routing, security, energy efficiency, attack resistance, authentication accuracy and computational efficiency in dynamic CRNs.

II. LITERATURE SURVEY

The literature review reveals that the current security solutions adopted by the CRN on communication, spectrum sensing and routing include the use of blockchain, AI, trust management, and cryptography. Yet they continue to have problems regarding high computational overhead, scalability, communication delay, limited adaptability, and lack of protection from new quantum challenges. Thus, a holistic solution, that combines the evaluation of trust, intelligent routing, route optimization, post-quantum encryption, zero-trust authentication and blockchain validation, is needed.

A. Blockchain Secure Communication

In order to transmit data securely while concealing it to the users, Chen et al. [6] presented a Blockchain Based Covert Communication Framework (BCCF), which combines information embedding technique, transaction filtering and transaction obfuscation technique into blockchain. The structure enhances privacy, reliability and anti-traceability using decentralized blockchain storage. But it has a very high transaction cost, communication latency, scalability problem and no adaptive threat detection mechanisms.

To overcome the security constraints of traditional covert communication, Onaji et al. [7] proposed an Adaptive AI-Driven Threat Intelligence and Blockchain-Assisted Trust Management (AITI-BTM). The system integrates threat intelligence, built using Deep Learning (DL), with permissioned blockchain trust management to identify threats, assess trust, and make secure communication decisions. It does, however, have high computation complexity, has to rely on large threat datasets, has to process overhead, and has to adapt in real time which is hard.

To enhance the secure communication in the future network, Zuo et al. [8] proposed an outline named Blockchain and Artificial Intelligence Enabled 6G Communication (BAI-6G). The structure combines blockchain-based authentication, privacy protection, and AI-driven network optimization, resource management, and intelligent decision-making. But the system is energy-intensive, AI blockchain integration is complex, scalable issues and communication latency issues arise.

To provide better privacy-preserving communication, Yadulla et al. [9] introduced Blockchain-Based Secure Covert Communication Framework (BSCCF) that exploits the blockchain characteristics of anonymity, tamper resistance and decentralization to build secure covert channels. The structure enhances the reliability of communication and the transmission of hidden information. It has some drawbacks, such as high storage cost, slow transaction speed, communication expense, and poor scalability in large network.

To prevent content tampering in metaverse communication, Lin et al. [10] designed an AI-generated Content (AIGC) protection system by combining Blockchain and Secure Semantic

Communication (BSSC-AIGC). In this structure, semantic communication, blockchain verification, and zero-knowledge proof mechanisms are integrated to provide verification of content and to resist malicious semantic attacks. It has a high

computational complexity, requires semantic processing overhead, has issues with scalability of the blockchain, and is not very flexible in handling advanced attacks.

Table 1. Analysis of DL -Based Blockchain Secure Communication System

Ref. No	Study	Domain	Approach	Analysis	Limitations
11	R. Kumar et al. (2022)	Zero Touch Networks	DL - and Blockchain-Assisted Secure Zero Touch Network (DLB-ZTN)	Combines VAE-AGRU, blockchain, smart contracts, ECC, and PoA for intrusion detection and secure data sharing.	High computational complexity, blockchain overhead, and scalability issues.
12	M. R. H. Talpur et al. (2021)	Secure Communication	AI and Blockchain-Based Secure Inter-Institutional Communication Model (AIB-SICM)	Integrates AI, blockchain, biometric authentication, and credential verification for secure inter-institutional communication.	Authentication delay, storage overhead, and limited intelligent threat detection.
13	Z. Chen et al. (2022)	CRNs	Blockchain-Based Distributed Spectrum Database (BC-DSDB)	Uses MAD estimation, POHC consensus, and SRC for secure spectrum management and dynamic spectrum allocation.	Consensus latency, storage overhead, and scalability limitations.
14	Z. Xiandong et al. (2025)	Spectrum Sensing	Two-Stage Consensus and Storage Optimization (TSCSO)	Employs IMAS-based two-stage consensus and storage optimization to reduce communication and storage overhead.	Cryptographic complexity, communication delay, and limited adaptive intelligence.
15	E. Ezhilarasi et al. (2024)	Cognitive Radio Security	Robust Cooperative Spectrum Sensing using SHA-3 (RCSS-SHA3)	Combines SHA-3 hashing, blockchain, and energy detection to detect malicious users during spectrum sensing.	High computation cost, energy consumption, and blockchain processing overhead.

The Analysis of DL Structure is summarized in Table 1 where the application domains, techniques integrated, security approaches and limitations of various structure are presented.

B. Deep Learning-Enabled Secure Communication in CRNs

Marriwala et al. [16] suggested a Blockchain-Based Dynamic Spectrum Sensing Framework with Node Evaluation and Selection (B-DSS-NES) for secure

spectrum management in CRNs. The system introduces Node Evaluation and Selection (NES) and blockchain based secure spectrum sensing approaches, for selecting reliable sensing nodes and minimizing the attacks from malicious nodes. It has, however, the drawbacks of blockchain overhead, complexity in communication, as well as scalability issues.

Awan et al. [17] presented a Blockchain Based Secure Routing and Trust Management (BSRTM) in wireless sensor networks. The combination of

blockchain authentication, trust evaluation, Rivest–Shamir–Adleman (RSA) encryption, and energy-aware routing is utilized to detect malicious nodes and prevent data from being compromised. It does have high encryption complexity, energy usage, and blockchain processing overhead, however.

Wu et al. [18] proposed a Blockchain-Driven Wireless Resource Management (BD-WRM) for the next-generation wireless networks. The structure incorporates blockchain, optimization models, game theory, auction mechanisms, and machine learning to effectively allocate resources and manage the spectrum. It has a high integration complexity, consensus latency and scalability issues, however. Sharma et al. [19] introduced a Blockchain Based Secure Community Interaction (BSCI) that ensures secure and transparent communication between

communities by leveraging a tamper-proof blockchain ledger, Replicated and Fault-Tolerant (RAFT) consensus, and key management. But there is there a storage overhead, key management complexity and communication delay issues with the structure. Qiu et al. [20] proposed Blockchain Privacy-Based Transfer Encoder Neural Network (BP-TENN) for cognitive network optimization and predictive analysis. The system incorporates blockchain privacy protection and transfer encoder neural networks, Binary Swarm Optimization (BSMO) and Artificial Neural Network (ANN) for spectrum prediction and Quality of Service (QoS) enhancement. It has a very high model training complexity, optimization overhead and a lack of adaptability to dynamic network environments.

Table 2. Comparative Analysis of Blockchain-Based Secure Spectrum Sensing Techniques in CRNs

Ref. No	Author et al.	Year	Scenario	Classification Method	Limitations	Future Research Direction
21	Vedachalam et al.	2024	CRN Spectrum Sensing Data	Adjustable Trainable Sigmoid Nesterov-accelerated Recurrent Neural Network, Format Pareto Preserving Distributed Encryption Standard (ATSNRNN-enabled FPPDES) with ML	High computation and encryption overhead.	Lightweight AI-based secure sensing models.
22	Khanna et al.	2022	CRN Spectrum Sensing Environment	Blockchain-Based Security Enhancement and Spectrum Sensing Framework	High latency and storage cost.	Lightweight blockchain consensus mechanisms.
23	Balakumar and Sendrayan	2023	Cooperative Spectrum Sensing Dataset	Blockchain-Based Cooperative Spectrum Sensing (BC-CSS)	Communication overhead and scalability issues.	Optimized blockchain-based sensing approaches.
24	Helmy et al.	2022	Cognitive Radio Spectrum Allocation Scenario	Spectrum Allocation Optimization Techniques	Limited security and threat detection.	AI-driven secure spectrum allocation.
25	Duraisamy et al.	2022	Cognitive Radio Blockchain	Certificateless Linkable Ring Signature-Based	High cryptographic computation cost.	Efficient lightweight authentication methods.

			Network	Blockchain Framework (CLRS- BC)		
--	--	--	---------	---------------------------------------	--	--

Table 2 shows the comparative analysis of secure spectrum sensing techniques based on the blockchain technology with the applied scenarios, proposed methods, limitations and future research directions. The analysis shows how security has been improved, and raises issues regarding scalability, computation efficiency and adaptive communication.

C. Blockchain Applications in CRNs

In this research, Jayatunga et al. [26] proposed Blockchain-Based Security Framework for Wireless and Cognitive Networks, which discussed the applications of blockchain in WSNs, CRNs, SDNs, opportunistic mobile networks, and delay-tolerant networks. The system emphasizes on blockchain-based authentication, privacy safeguarding, and secure data handling processes. It, however, is costly in terms of computation, requires high scalability, and has consensus delay in resource-constrained networks.

In CRNs, Rajesh Babu and Amutha [27] suggested a new Blockchain and Extreme Learning Machine-Based Spectrum Management Framework (BC-ELM-SM). The proposed structure combines blockchain technology and the Extreme Learning Machine (ELM) to improve the spectrum allocation, security, and intelligent decision-making process. It does have training complexity, blockchain overhead and limited adaptability to dynamic spectrum environment, though.

Sundar and Senthilkumar [28] proposed a Regressive Schnorr Signature-Based Deep Belief Secure Data

Routing Framework (RSS-DB) for a CRN. It is a combination of Schnorr signature-based authentication and Deep Belief Networks (DBN) for secure routing and data protection. However, it has high cryptographic computation and complicatedness of the model.

The Artificial Neural Network-Based Secure Handoff Framework (ANN-SHF) for CRNs was suggested by Rathee et al. [29]. The structure introduces artificial neural networks to enhance the security of handoff and to identify possible threats during the spectrum mobility. But it has a high training requirement, computational complexity and dependence on the quality of the training data.

Saravanan et al [30] proposed a Two-Level Shared Key Authentication Based Secure Channel Estimation Model (TLSK-SEC) for the physical layer security in CR. Two-level shared key authentication is used in the model to improve secure channel estimation, guarantee the security of the communication channel. But there are some problems of management complexity and communication overhead.

Tolley [31] explored the problems of Security and Reliability Enhancement Frameworks for Crowdsourced Spectrum Access Systems and CRNs. The research in this concerned with the enhancement of secure sharing, reliability and ability to defend against unauthorized access in the spectrum. But it will need sophisticated adaptive security mechanisms and effective threat detection for deployments on a large scale.

Table 3. Analysis of Attack Mitigation Strategies in CRNs

Ref. No	Author et al.	Year	Attack Type	Proposed Technique	Key Contribution	Research Gap
32	Ezhilarasi et al.	2023	Spectrum sensing attacks, malicious user attacks, and network security threats	Machine Learning and Blockchain-Based Attack Mitigation Framework	Reviews ML and blockchain solutions for detecting and mitigating CRN attacks while improving secure spectrum sharing.	Lacks practical implementation and real-time adaptive defense mechanisms.
33	Saraswathi	2025	Severity-based	Blockchain and	Uses blockchain	High computational

	and Dayana		CRN attacks	Gaussian Fuzzy Hyper Quadratic Distance Classifier (GFHQDC-Based Attack Mitigation System)	security and GFHQDC optimization to classify attack severity and improve mitigation performance.	overhead and scalability challenges in large CRNs.
34	Zamanian et al.	2021	Jamming attacks in Massive MIMO CRNs	Optimized Jamming Attack Model	Develops an optimization-based analysis of jamming attacks to evaluate vulnerabilities in CRNs.	Focuses mainly on attack modeling with limited intelligent protection strategies.

Table 3 illustrates the analysis of attack mitigation techniques in CRNs, their security issues, proposed techniques, contributions, and limitations.

Aslam et al. [35] presented a security framework for the 6G CRN (6G-CRN) which discusses applications, enabling technologies and security challenges of 6G CRN, leveraging the support of AI, dynamic spectrum access, big data analytics, mmWave, and THz communication. It states that, in the future, 6G networks will include cognitive radios that reach peak data rates of up to 1 Tbps, end-to-end latency of less than 1 ms, spectral efficiency of up to 1000 bps/Hz and mobility support up to 1000 km/h.

III. PROPOSED METHODOLOGY

Figure 2 illustrates the overall workflow of the proposed CognitiveTrust-PQZTA framework for secure and adaptive routing in CRNs. First, the node behavior and residual energy, packet forwarding information, spectrum access behavior, communication relationships, and historical reputation data of the CRN network are collected and processed via the TFTERN.

The TFTERN takes the weighted consideration of the temporal trust and reputation of CRN nodes under the consideration of the availability of their energy and

behavioral consistency. The trust information is then passed to TGAT that learns the dynamic spatial-temporal relationship between the CRN nodes and selects trustworthy candidate communication paths. Later, the AM-MRMO technique is used to optimize the candidate routes, taking into account various parameters, including hop count, delay, energy, routing overhead, malicious-node exposure, path reliability, and spectrum stability.

The optimized communication paths are then securely established via the PAEKHE mechanism, which creates secure session keys and shields transmitted data from current and future quantum threats. The CRAZTA mechanism continually analyzes the trustworthiness of entities based on the context, deviations from that context, and the history of communications. Lastly, the RA-PoA-BFT mechanism uses a blockchain consensus algorithm to validate authentication and routing transactions in a decentralized way.

Accordingly, the proposed architecture combines the four features of trust evaluation, intelligent routing, route optimization, post-quantum security, continuous authentication, and blockchain-based validation to ensure secure, reliable, and adaptive CRN communication.

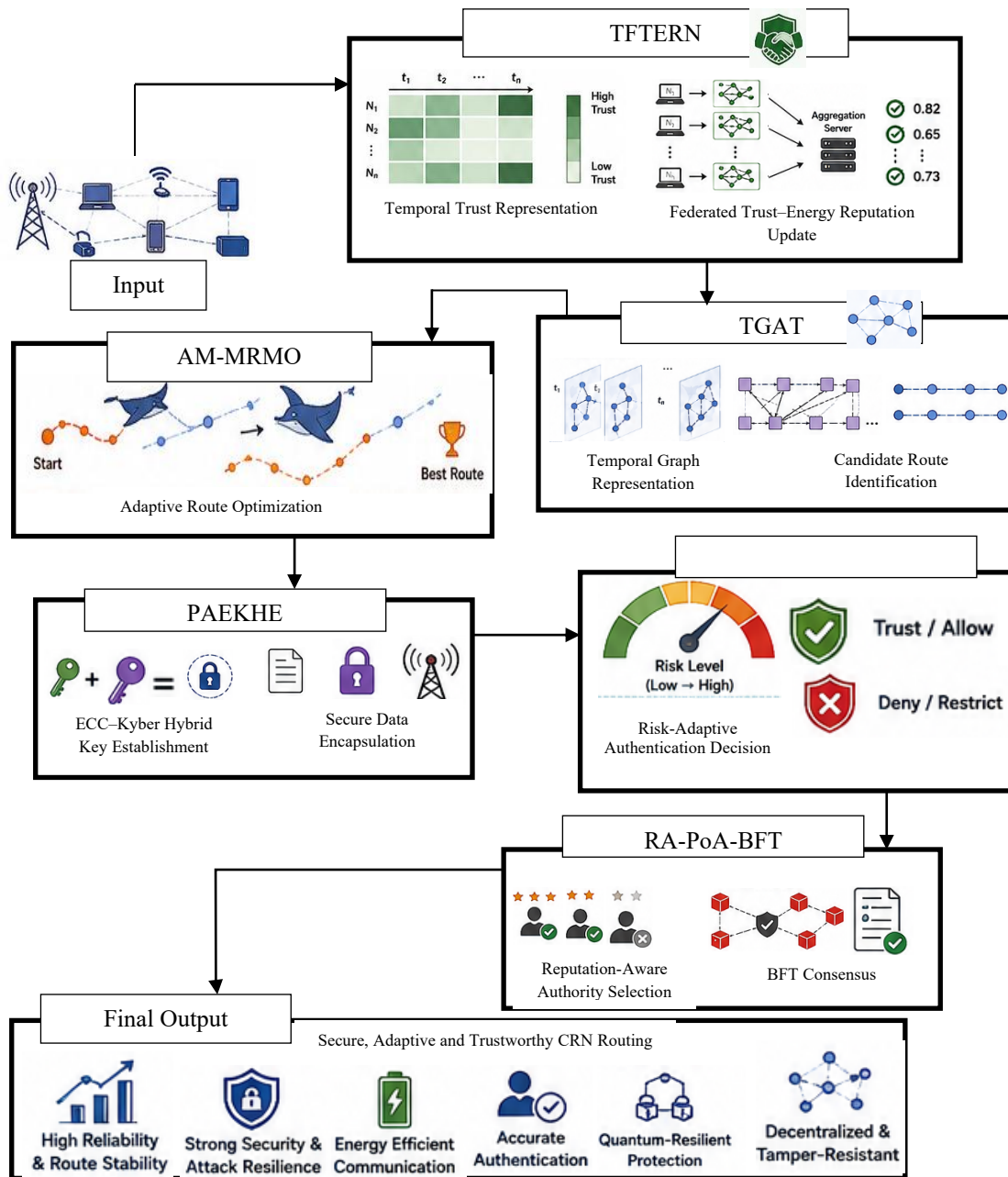


Figure 2. Architecture of the Proposed CognitiveTrust-PQZTA Secure Routing

A. Temporal Federated Trust-Energy Reputation Network (TFTERN)

The TFTERN first forms a temporal trust representation for every CRN node based on the successive communication observations. The node observations are presented in a way that accounts for the progression of behavior over time, by presenting them according to the communication intervals. The federated learning process then completes the local

trust computation at participating nodes and merges the local trust information to form a joint representation of trust information. The node reputation is updated based on changes over time in the local values of the trust, so as to take into account the trust that the nodes had in the past, despite changes in values, and also to incorporate the current behavior of the nodes. The new trust representation is merged with relation to trust and energy to

distinguish stable and unstable nodes. TFTERN finally returns an updated Trust value for each node participating in the protocol, which is provided to TGAT as a trust value of each node for future candidate-routes identification.

This below equation 1 computes the current time t value of trust at the current node. The $T_i^{(t)}$ – previous trust value and $L_i^{(t)}$ –trust value estimated by the node based on its own observations. This parameter α influences the impact of the previous trust information.

$$T_i^{(t)} = \alpha T_i^{(t-1)} + (1 - \alpha) L_i^{(t)} \quad (1)$$

The higher the α , the more weight is placed on historical trust and the lower the α , the more weight is placed on the recent behavior. Thus, this equation can be used to model the temporal variation of node trust in TFTERN.

The below equation 2 calculates the federated trust value T_i^F for node i based on the trust value information from k of the participating clients/nodes.

$$T_i^F = \sum_{k=1}^K \frac{n_k}{\sum_{j=1}^K n_j} T_{i,k} \quad (2)$$

The local trust value $T_{i,k}$ is computed by the local participant k and n_k is the number of observations relevant to the participant K . The weighted aggregation creates a collective trust representation without having to share individual raw observations.

The final TFTERN trust/reputation score R_i –obtained by this equation 3. The federated trust value is T_i^F , the normalized residual-energy information is E_i and the historical reputation is H_i .

$$R_i = \beta T_i^F + (1 - \beta)[\gamma E_i + (1 - \gamma)H_i] \quad (3)$$

Parameters β and γ determine the relative amount of federated trust and energy condition and historical reputation, respectively. The output of TFTERN is then a final node trust/reputation R_i –passed to TGAT for the aim of identification of reliable candidate routes.

B. Temporal Graph Attention Transformer (TGAT)

The trust scores obtained from TFTERN are fed into the TGAT to find reliable candidate communication paths. The initial representation of the CRN is as a dynamic graph, with nodes corresponding to cognitive radio devices and communication links representing possible interactions between nodes. The temporal graph representation is built using the features of the nodes and the TFTERN trust values.

Then, TGAT records the variations in node relationships over various communication time instances with temporal information. The graph-attention mechanism gives more weight to the adjacent nodes based on their trust and communication relationships, such that confident nodes and links are assigned more weights to be the focus of representation learning.

The transformer block also captures the long-range dependencies between nodes and learns the changing spatial-temporal structure of the CRN. TGAT then analyses the representations of the nodes and links and proposes the possible node-to-node connections, creating reliable candidate communication paths. Each such path is subsequently relayed to AM-MRMO where a multi-objective routing optimization is carried out. The primary product of TGAT is therefore a collection of reliable candidate routes, instead of the final optimized route.

The temporal representation of CRN node i – time t – created by the above equation 4. This X_i^t –current node features, R_i –trust/reputation score retrieved from TFTERN and τ_i^t – temporal information of the node.

$$h_i^t = W_h [X_i^t \| R_i \| \tau_i^t] + b_h \quad (4)$$

These three pieces are concatenated together using the concatenation operator $\|$ to form a single representation of the input. The W_h and b_h are the weight and bias parameters that are learned. Hence, it combines nodes features, trust information and temporal behaviors into one node representation for the use of TGAT.

The below equation 5 is used to update the representation of node, given information from neighbouring nodes. The N_i –neighboring nodes of i , while h_j^t is the temporal representation of neighbor j .

$$z_i^t = \sigma(\sum_{j \in N_i} \alpha_{ij}^t W_z h_j^t) \quad (5)$$

The attention coefficient α_{ij}^t –weight to communication relationships that are relevant and reliable, and helps to incorporate TGAT into the models. W_z – weights of the z – transform and σ – activation function. The updated representation of the

spatial-temporal node is z_i^t , which is then utilized for finding reliable candidate-routes.

C. Adaptive Multi-Objective Manta Ray Optimization (AM-MRMO)

The candidate routes produced by TGAT are given to AM-MRMO method to determine most appropriate communication route. AM-MRMO represents each route that the candidate wants to take as a solution and rates it based on several routing goals. The optimization algorithm takes into account, among others, hop count, communication delay, energy consumption, routing overhead, malicious-node exposure, path reliability and spectrum stability. The goals are mutually assessed to ensure that the route is not optimal for one goal but sub-optimal for another. The adaptive optimization process optimizes the candidate solutions and looks for better route configurations based on the sum of the objective values. In all iteration poorer routes are replaced or improved with better routes and viable communication paths are maintained. The optimization process continues until the stopping condition is met and optimal solution is gained. The results of AM-MRMO are the optimized communication route that is then handed over to PAEKHE for secure session-key establishment and data protection.

This below equation 6 is used for updating the position of candidate route in the optimization process of AM-MRMO. It X_i^t –represents the i – th candidate route and X_{best}^t – route found in the t -th iteration.

$$X_i^{t+1} = X_{best}^t + r(X_{best}^t - X_i^t) \quad (6)$$

The parameter r –adaptive movement of the candidate solution. The new position X_i^{t+1} – pushes the candidate towards the solution that is found to be promising, allowing AM-MRMO to explore a better communication path. This process is then repeated until the optimum possible route is achieved, which is then passed along to PAEKHE.

This below equation 7 is used to update the candidate route P_i during the AM-MRMO optimization process. The $P_i^{(t)}$ is the best route candidate found up to iteration t and $P_{best}^{(t)}$ –route found so far.

$$P_i^{(t+1)} = P_i^{(t)} + \lambda_t(P_{best}^{(t)} - P_i^{(t)}) \quad (7)$$

The adaptive factor λ_t determines strongly the candidate route gets modified towards the best route. The improved candidate route of next iteration is $P_i^{(t+1)}$, AM-MRMO repeatedly searches for the best possible communication route, and then PAEKHE securely communicates through the route.

D. Post-Quantum Adaptive ECC–Kyber Hybrid Encryption (PAEKHE)

The optimized route found by AM-MRMO is sent to PAEKHE for setting up a secure communication session. PAEKHE is a hybrid key protection with ECC-based cryptographic operations and Kyber post-quantum mechanism. The ECC component is used for efficient key establishment and Kyber is used for protection from possible quantum attacks. The proactive mechanism decides which hybrid cryptographic operation is suitable for optimized route based on the communication requirements.

The shared secret generated is then used to set up a secure session, and the data being communicated is encrypted prior to sending it down the chosen path. On the receiver end, the same hybrid process is used to extract the common secret and to access the data securely. So, PAEKHE output is a secure session key and protected communication data that are then managed in the CRAZTA-based continuous authentication process.

$$K_H = H(K_{ECC} \| K_{Kyber}) \quad (8)$$

The above equation 8 operator combines both secrets, and $H(.)$ –cryptographic hash function that generates a single key from the combined secrets. This combination gives the session both securities based on ECC and post-quantum security using Kyber. The generated is then to be used for secure communication.

$$C = Enc_{K_H}(M) \quad (9)$$

This above equation 9 used to encrypt the initial message M with the hybrid session key K_H . The plaintext message m is encrypted by Enc and yields the ciphertext C , which ensures that the information sent through can't be accessed by unauthorized parties. The Cipherized Text is sent along the AM-MRMO optimized route and processed by the CRAZTA which provides ongoing risk adaptive authentication.

E. Continuous Risk-Adaptive Zero-Trust Authentication (CRAZTA)

The protected communication session created by PAEKHE is continually monitored by the proposed CRAZTA mechanism. CRAZTA assesses the level of risk of communicating entities based on their current authentication state, and on the behavioral deviations during communication. The risk assessment is not based on an individual authentication decision, but is continually updated. If the observed behavior is still in line with the expected behavior, then the entity resumes the communication session. When considerable behavioral differences are observed, the risk level of the entity is raised and the authentication is adjusted accordingly. By continuously monitoring, CRAZTA allows to detect potentially compromised or abnormal entities during the active session. The final result of CRAZTA is an updated entity-risk value and an authentication decision which is sent to RA-PoA-BFT for decentralized authentication and routing transaction validation.

The below equation 11 compute the behavioral deviation D_i^t of entity at time i . This B_i^t –actual behavior and B_i^{ref} –reference behavior which is desired.

$$D_i^t = \|B_i^t - B_i^{ref}\| \quad (11)$$

The norm is a measure of the difference. Sums that are higher than the value for D_i^t –signal a more significant deviation and/or abnormal behavior.

$$Q_i^t = \alpha Q_i^{t-1} + (1 - \alpha) D_i^t \quad (12)$$

This above equation 12 is updated for the risk score Q_i^t – entity i continually. It Q_i^{t-1} –previous value of risk and D_i^t – current value of behavioral deviation. The α –parameter which dictates the effect of historical risk. Therefore, the current risk is a result of combining past and current risk with past and current behavior (CRAZTA).

The authentication decision A_i^t –produced by this equation 12 on the basis of the risk score that is currently present, θ – predetermined risk threshold. If Q_i^t – acceptable range then the entity is still authenticated.

$$A_i^t = \begin{cases} 1, & Q_i^t \leq \theta \\ 0, & Q_i^t > \theta \end{cases} \quad (13)$$

If the risk is higher than the threshold θ , the authentication is rejected or it needs to be re-authenticated. The updated risk score and

authentication decision is then the final CRAZTA output and can be passed on to RA-PoA-BFT.

F. Reputation-Aware Proof-of-Authority Byzantine Fault-Tolerant (RA-PoA-BFT)

The authentication and routing information generated by CRAZTA is sent to RA-PoA-BFT for decentralized validation. The first step of RA-PoA-BFT is to set up the eligibility of the authority nodes that participate. The chosen authorities confirm the coming in authentication and routing transactions and are involved in the Proof-of-Authority consensus process. The Byzantine Fault-Tolerant mechanism can help the network arrive at a consistent decision in the event that some of the authorities involved act incorrectly. Valid transactions are taken and added to the decentralized blockchain, and invalid or inconsistent transactions are rejected. So, the final validated authentication and routing transaction is generated by RA-PoA-BFT, thus completing the secure routing process.

The below equation 14 chooses the eligible authority nodes based on reputation, in reputation score of nodes v_i – denoted as Rep_i and the minimum reputation threshold is denoted as θ_R .

$$A = \{v_i | Rep_i \geq \theta_R\} \quad (14)$$

The nodes whose reputation meets the threshold become a set called A, which is an authority set. If the reputation of a node meets the threshold, the node becomes a node in an authority set A. This guarantees only well-known nodes are involved with validating transactions.

$$V(T) = \frac{\sum_{i=1}^N w_i v_i(T)}{\sum_{i=1}^N w_i} \quad (15)$$

The above equation 15 for calculating aggregated validation value $V(T)$ for the transaction T , where $v_i(T)$ –validation decision of the authority i , and w_i is the reputation-based weight of that authority. The weighted aggregation decides if the authentication or routing transaction gets enough authority support.

This below equation 16 decides whether the transaction is able to get BFT consensus or not. The N –number of validators participating and f is the greatest number of Byzantine/faulty validators.

$$\sum_{i=1}^N v_i(T) \geq 2f + 1 \quad (16)$$

Once $2f + 1$ validators approve the transaction, the transaction is accepted and added to the blockchain. Therefore, RA-PoA-BFT's final product is the authenticated and routed transaction.

IV. RESULTS AND DISCUSSION

This section analyzes the performance of the BCCF, BSSC-AIGC, RCSS-SHA3, and proposed method by considering various communication and security performance metrics. The comparison is performed in the CRN to evaluate the secure communication effectiveness with blockchain. In addition, the proposed framework is studied with the help of Packet Delivery Ratio (PDR), Energy Efficiency, Security Performance, Authentication Rate, Throughput, and End-to-End Delay. The proposed method's ability to ensure reliable, secure, and efficient communication is also verified by comparing the performance of the proposed method with the performance of existing blockchain-based secure communication methods through these performance metrics, while also enhancing the network performance and decreasing the communication overhead.

Table 4. Performance Metrics for Blockchain-Based Secure Communication in CRNs

Performance Metric	Mathematical Expression
Packet Delivery Ratio (PDR)	$PDR = \frac{P_r}{P_s} \times 100$
Energy Efficiency (EE)	$EE = \frac{D_s}{E_c}$
Security Performance (SP)	$SP = \frac{A_d}{A_t} \times 100$
Authentication Rate (AR)	$AR = \frac{U_a}{U_t} \times 100$
Throughput (TP)	$TP = \frac{P_r \times P_{size}}{T}$
End-to-End Delay (EED)	$EED = \frac{1}{N} \sum_{i=1}^N (T_{ri} - T_{si})$

Table 4 shows the performance metrics considered for assessing the secure communication in CRNs using blockchain. These are measures of communication reliability, security, authentication and efficiency of the network.

Table 5. Simulation Parameter

Parameters	Values
Simulation Tool	Python
Network Area	1000 × 1000 m ²
Number of Cognitive Radio Nodes	50 – 500
Number of Primary Users	10
Number of Secondary Users	40 – 490
Communication Channel	Wireless Channel
Initial Energy	100 J
Packet Size	512 Bytes
Transmission Range	250 m
Simulation Time	100 sec
Spectrum Type	Dynamic Spectrum

The values of the simulation parameters used for the performance analysis are provided in Table 5. These are parameters that indicate the topology of the network, the configuration of their nodes and the circumstance of communication.

Table 6. Comparison of PDR and Energy Efficiency

Method	PDR (%)	Energy Efficiency (%)
BCCF (6)	83.45	82.76
BSSC-AIGC (10)	87.62	86.95
RCSS-SHA3 (15)	91.28	90.54
RA-PoA-BFT	96.15	95.38

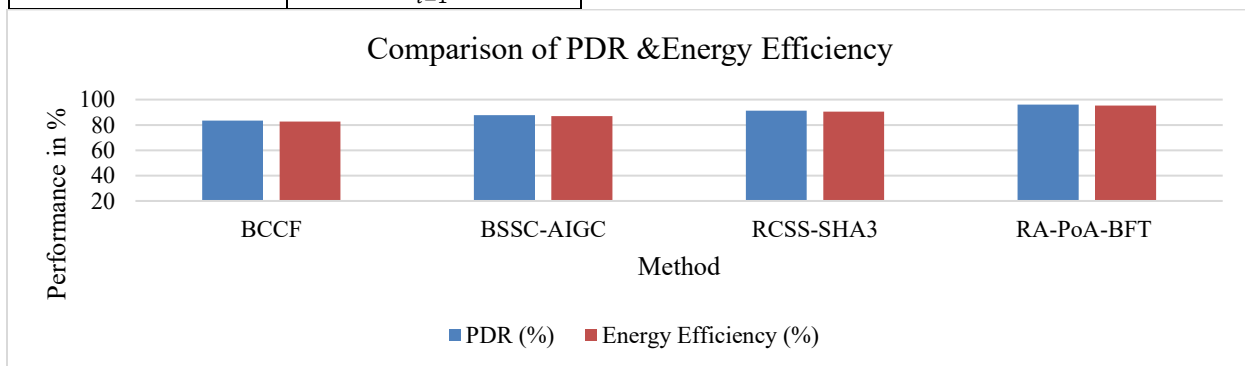


Figure 3: Comparison of PDR and Energy Efficiency

As shown in Table 6 and Figure 3, the PDR and Energy Efficiency of blockchain-based secure communication in CRNs has been compared. The results of this review are found to be: PDR values of BCCF, BSSC-AIGC, RCSS-SHA3 and RA-PoA-BFT are 83.45%, 87.62%, 91.28% and 96.15% respectively and the Energy Efficiency values are 82.76%, 86.95%, 90.54% and 95.38% respectively. The proposed method presents the best

communication reliability and energy use among all the compared methods.

Table 7. Comparison of Security Performance

Method	Security Performance (%)
BCCF (6)	85.84
BSSC-AIGC (10)	89.63
RCSS-SHA3 (15)	92.48
RA-PoA-BFT	95.76

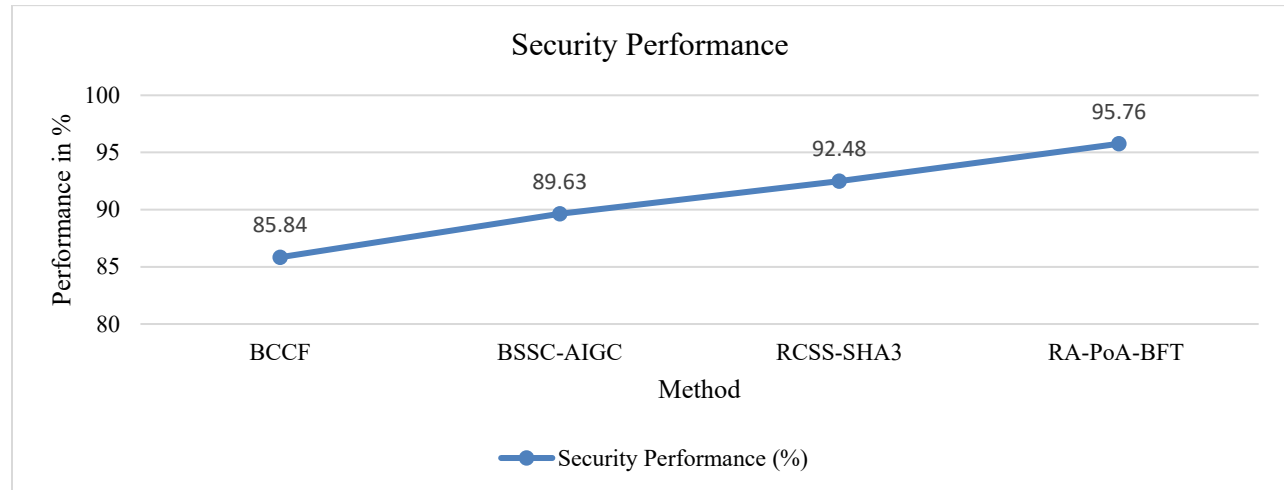


Figure 4: Analysis of Security Performance

Table 7 and Figure 4 compare the Security Performance of the BCCF, BSSC-AIGC, RCSS-SHA3 and the proposed method in CRNs. The security performance values of BCCF, BSSC-AIGC and RCSS-SHA3 methods are 85.84%, 89.63% and 92.48%, respectively, and the RA-PoA-BFT has the highest value of 95.76% compared to other methods. The better performance shows that the system is more protected from malicious attacks, it is more

secure, and it provides more reliable communication between users in CRNs using blockchain technology.

Table 8. Comparison of Authentication Performance

Method	Authentication (%)
BCCF (6)	83.18
BSSC-AIGC (10)	88.46
RCSS-SHA3 (25)	92.74
RA-PoA-BFT	95.99

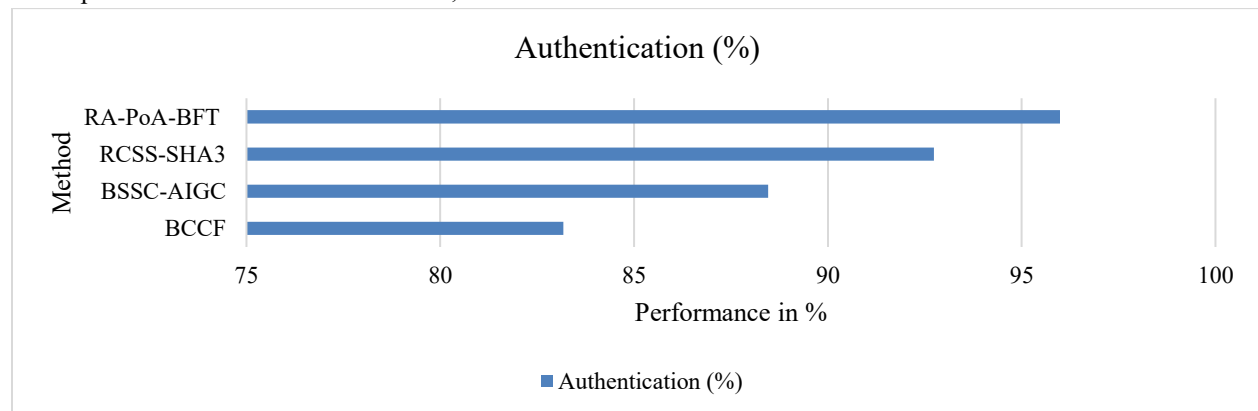


Figure 5: Analysis of Authentication performance

In CRNs, this research compares the Authentication Performance of the BCCF, BSSC-AIGC, RCSS-SHA3 and the RA-PoA-BFT as shown in Table 8 and Figure 5. In comparison with the BCCF, BSSC-AIGC and RCSS-SHA3, the RA-PoA-BFT was able to achieve the highest authentication performance of 95.99%, while BCCF, BSSC-AIGC and RCSS-SHA3 methods achieved the authentication rate of 83.18%, 88.46% and 92.74% respectively. This capability can be used to improve

secure user verification, trusted node validation, and reliable communication in CRNs.

Table 9. Comparison of Throughput

Method	Throughput (TPS)
BCCF (6)	142
BSSC-AIGC (10)	168
RCSS-SHA3 (15)	201
RA-PoA-BFT	245

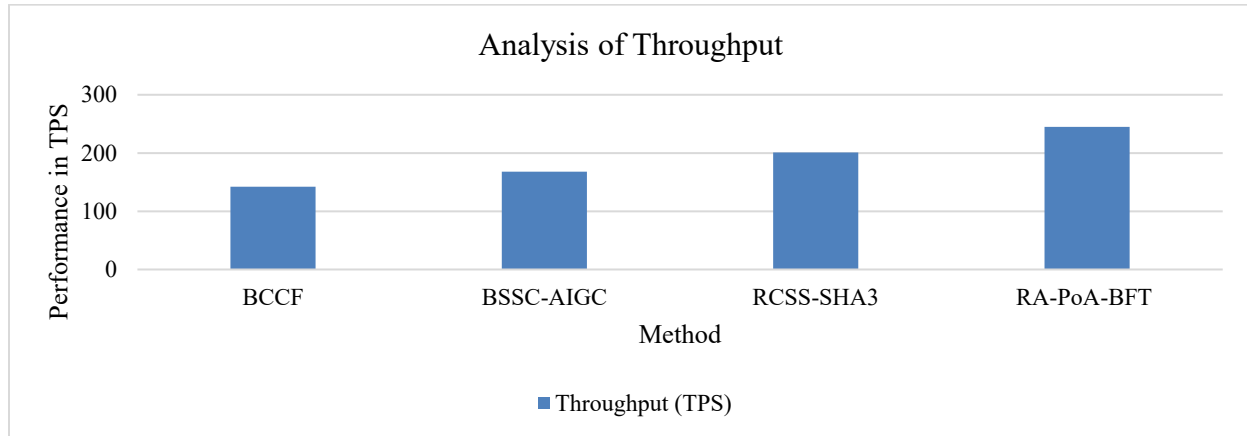


Figure 6: Analysis of Throughput

The performance comparison of BCCF, BSSC-AIGC, RCSS-SHA3 and RA-PoA-BFT in terms of Throughput (TPS) in CRN is shown in Table 9 and Figure 6. The RA-PoA-BFT has the highest throughput of 245 TPS while the BCCF method, BSSC-AIGC method, and RCSS-SHA3 method have 142 TPS, 168 TPS and 201 TPS respectively. The increased throughput reflects efficient blockchain

transaction processing, secure communication, and data transmission performance in CRNs.

Table 10. Comparison of End-to-End Delay

Method	End-to-End Delay (ms)
BCCF (6)	28.64
BSSC-AIGC (10)	22.83
RCSS-SHA3 (15)	16.75
RA-PoA-BFT	9.28

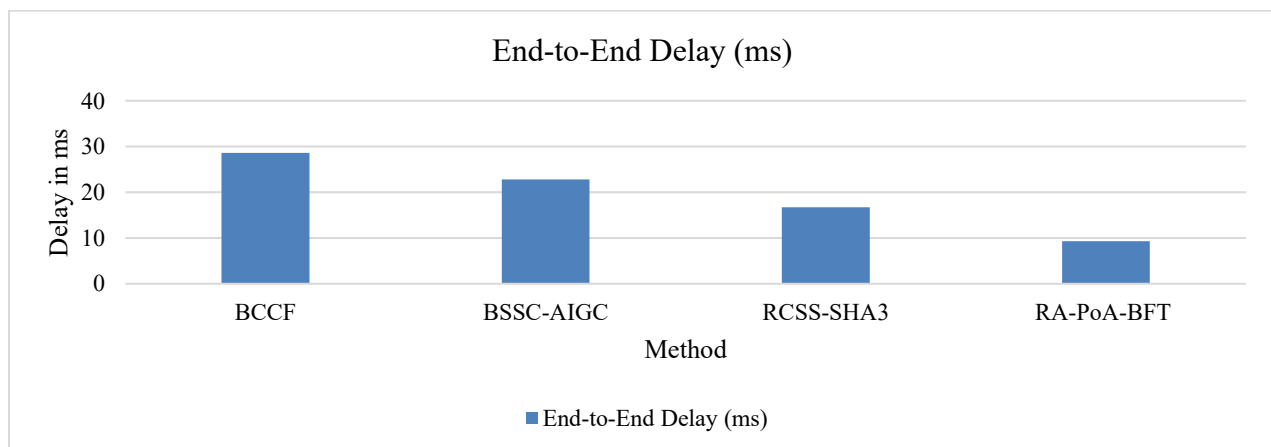


Figure 7: Analysis of End-to-End Delay

Table 10 and Figure 7 compare the End-to-End Delay of the BCCF, BSSC-AIGC, RCSS-SHA3 and the proposed method for the CRNs. The RA-PoA-BFT gives a delay of 09.28 ms while the BCCF, BSSC-AIGC method gives delay 28.64 ms, 22.83 ms respectively. This proves that the communication delay in the blockchain was lowered, blockchain transaction verification was made faster, spectrum utilization was made efficient, and secure communication was ensured in CRNs.

V. CONCLUSION

In conclusion, the present research proposed an intelligent CognitiveTrust-PQZTA framework for secure and adaptive routing in CRNs. The proposed framework combines the following technologies: TFTERN: Adaptive Trust Evaluation, TGAT: Dynamic Spatial-Temporal Route Prediction, AM-MRMO: Multi-objective Route Optimization, PAEKHE: Post-quantum Encryption, CRAZTA: Continuous Zero-trust Authentication, and RA-PoA-BFT: Decentralized Blockchain Validation. TFTERN finds reliable nodes using behavioral, energy, forwarding, spectrum-access, and reputation information, while TGAT and AM-MRMO offer reliable and optimized communication paths in dynamic CRN conditions. PAEKHE mechanism reinforces data confidentiality against the emerging threats in quantum world while the node trustworthiness is continually verified in the CRAZTA and RA-PoA-BFT provides a secure and tamper-resistant transaction validation mechanism. The experimental results demonstrate that the proposed framework can achieve a PDR of 96.15%, energy efficiency of 95.38%, security performance of 95.76%, authentication performance of 95.99%, and end-to-end delay of 9.28 ms with a throughput of 245 TPS. As a result, the outcomes show a higher reliability, security, energy saving, authentication, transaction processing and delay performance than the current approaches. The proposed CognitiveTrust-PQZTA is a complete, scalable and robust framework to secure next-generation cognitive wireless communication. Further improvements to post-quantum cryptographic and adaptive routing mechanisms, along with the deployment of CRN and making it lightweight on resource-constrained nodes,

and large-scale network validation will continue to be studied in the future.

REFERENCES

- [1] Li, Xiao, and Weili Wu. "Recent advances of blockchain and its applications." *Journal of Social Computing* 3.4 (2022): 363-394.
- [2] Faheem, Muhammad, et al. "A lightweight smart contracts framework for blockchain-based secure communication in smart grid applications." *IET generation, transmission & distribution* 18.3 (2024): 625-638.
- [3] Chandan, Radha Raman, et al. "Secure modern wireless communication network based on blockchain technology." *Electronics* 12.5 (2023): 1095.
- [4] Mahvash, Mahsa, et al. "Blockchain-inspired trust management in cognitive radio networks with cooperative spectrum sensing." *Pervasive and Mobile Computing* 106 (2025): 101999.
- [5] El-Hajj, Mohammed. "Enhancing communication networks in the new era with artificial intelligence: techniques, applications, and future directions." *Network* 5.1 (2025): 1.
- [6] Chen, Zhuo, et al. "Blockchain meets covert communication: A survey." *IEEE Communications Surveys & Tutorials* 24.4 (2022): 2163-2192.
- [7] Vincent Onaji et al. "Adaptive AI-Driven Threat Intelligence and Blockchain-Assisted Trust Management for Secure and High-Integrity Communication Systems" *International Journal of Computer Applications Technology and Research* Volume 12–Issue 12, 323 – 340, 2023, ISSN: -2319–8656 DOI:10.7753/IJCATR1212.1029
- [8] Zuo, Yiping, et al. "A survey of blockchain and artificial intelligence for 6G wireless communications." *IEEE Communications Surveys & Tutorials* 25.4 (2023): 2494-2528.
- [9] Yadulla, Akhila Reddy, Bhargavi Konda, and Vinay Kumar Kasula. "Blockchain for secure communication." *Blockchain Applications for the Energy and Utilities Industry*. IGI Global Scientific Publishing, 2025. 103-140.
- [10] Lin, Yijing, et al. "Blockchain-aided secure semantic communication for AI-generated

- content in metaverse." IEEE Open Journal of the Computer Society 4 (2023): 72-83.
- [11] Kumar, Randhir, et al. "Deep-learning-based blockchain for secure zero touch networks." IEEE Communications Magazine 61.2 (2022): 96-102.
- [12] Talpur, Mir Rahib Hussain, et al. "A model for secure inter-institutional communication based on artificial intelligence (AI) and blockchain." Int. J. Comput. Intell. Control 13 (2021): 145-154.
- [13] Chen, Zhenjia, Lihui Wang, and Yonghui Zhang. "Blockchain structure electromagnetic spectrum database in distributed cognitive radio monitoring system." IEEE Transactions on Cognitive Communications and Networking 8.4 (2022): 1647-1664.
- [14] Xiandong, Zheng, Pan Zhiwen, and Liu Nan. "Optimization of two-stage consensus and storage of blockchain-based spectrum sensing in cognitive radio networks." IEEE Sensors Journal 25.13 (2025): 24431-24440.
- [15] Ezhilarasi, Evelyn, and J. Christopher Clement. "Robust Cooperative spectrum sensing in Cognitive Radio Blockchain network using SHA-3 algorithm." Blockchain: Research and Applications 5.4 (2024): 100224.
- [16] Marriwala, Nikhil Kumar, et al. "An analytical model for dynamic spectrum sensing in cognitive radio networks using blockchain management." Engineering Proceedings 59.1 (2024): 163.
- [17] Awan, Saba, et al. "Blockchain based secure routing and trust management in wireless sensor networks." Sensors 22.2 (2022): 411.
- [18] Wu, Meining, et al. "Blockchain-driven resource management in wireless communications and networks: Models, approaches, and applications." IEEE Communications Surveys & Tutorials (2025).
- [19] Sharma, Rahul, Mohammad Wazid, and Prosanta Gope. "A blockchain based secure communication framework for community interaction." Journal of Information Security and Applications 58 (2021): 102790.
- [20] Qiu, Ya-qin, and Chao Zhang. "Artificial intelligence driven cognitive optimization and predictive analysis using blockchain privacy-based machine learning model." Computers and Electrical Engineering 117 (2024): 109238.
- [21] Vedachalam, Saraswathi, and Dayana Raj. "Development of a privacy-preserved and secure cooperative spectrum sensing system in cognitive radio networks using ATSNRNN-enabled FPPDES with machine learning." IEEE Access 12 (2024): 155838-155850.
- [22] Khanna, Ashish, et al. "Blockchain-based security enhancement and spectrum sensing in cognitive radio network." Wireless Personal Communications 127.3 (2022): 1899-1921.
- [23] Balakumar, D., and Nandakumar Sendrayan. "Enhance the probability of detection of cooperative spectrum sensing in cognitive radio networks using blockchain technology." Journal of Electrical and Computer Engineering 2023.1 (2023): 8920243.
- [24] Helmy, Maram, Mohamed S. Hassan, and Mahmoud H. Ismail. "Spectrum allocation techniques for cognitive radio networks." IEEE Access 10 (2022): 28180-28193.
- [25] Duraisamy, Abitha Kumari, et al. "Certificateless linkable ring signature-based blockchains for securing cognitive radio networks." Concurrency and Computation: Practice and Experience 34.24 (2022): e7235.
- [26] Jayatunga, Eranda Harshanath, Pasika Sashmal Ranaweera, and Indika Anuradha Mendis Balapuwaduge. "Blockchain advances and security practices in WSN, CRN, SDN, opportunistic mobile networks, delay tolerant networks." Revolutionary Applications of Blockchain-Enabled Privacy and Access Control. IGI Global, 2021. 1-34.
- [27] Rajesh Babu, C., and B. Amutha. "Blockchain and extreme learning machine-based spectrum management in cognitive radio networks." Transactions on Emerging Telecommunications Technologies 33.10 (2022): e4174.
- [28] Sundar, T., and A. Senthilkumar. "Regressive Schnorr Signature Based Deep Belief for Secured Data Routing In Cognitive Radio Network." National Journal of Antennas and Propagation (2026): 131-143.
- [29] Rathee, Geetanjali, et al. "Handoff security using artificial neural networks in cognitive radio networks." IEEE Internet of Things Magazine 3.4 (2021): 20-28.
- [30] Saravanan, K., et al. "Secure channel estimation model for cognitive radio network physical layer

security using two-level shared key authentication." *Scientific Reports* 15.1 (2025): 2445.

- [31] Tolley, Joseph D. "Improvements to Enhance The Security and Reliability of Crowdsourced Spectrum Access Systems and Cognitive Radio Networks." (2025).
- [32] Ezhilarasi, I. Evelyn, J. Christopher Clement, and Joseph M. Arul. "A survey on cognitive radio network attack mitigation using machine learning and blockchain." *EURASIP Journal on Wireless Communications and Networking* 2023.1 (2023): 98.
- [33] Saraswathi, Vedachalam, and R. Dayana. "Development of a Severity-Based Attack Mitigation System in Cognitive Radio Networks Using Blockchain and GFHQDC." *IEEE Access* 13 (2025): 51765-51780.
- [34] Zamanian, S. Fatemeh, et al. "Attacking massive MIMO cognitive radio networks by optimized jamming." *IEEE Open Journal of the Communications Society* 2 (2021): 2219-2231.
- [35] Aslam, Muhammad Muzamil, et al. "Sixth generation (6G) cognitive radio network (CRN) application, requirements, security issues, and key challenges." *Wireless Communications and Mobile Computing* 2021.1 (2021): 1331428.