IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 14 November 2023, accepted 29 December 2023, date of publication 8 January 2024, date of current version 22 January 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3350739

RESEARCH ARTICLE

BSMACRN: Design of an Efficient Blockchain-Based Security Model for Improving Attack-Resilience of Cognitive Radio Ad-hoc Networks

DEBABRATA DANSANA[1], PRAFULLA KUMAR BEHERA[1], S. GOPAL KRISHNA PATRO[2], QUADRI NOORULHASAN NAVEED[3], AYODELE LASISI[3], AND ANTENEH WOGASSO WODAJO[4]

[1]Department of Computer Science and Applications, Vani Vihar, Utkal University, Bhubaneswar, Odisha 751004, India
[2]School of Technology, Woxsen University, Hyderabad, Telangana 502345, India
[3]Department of Computer Science, College of Computer Science, King Khalid University, Abha 62529, Saudi Arabia
[4]Department of Automotive Engineering, College of Engineering and Technology, Dilla University, Dilla 419, Ethiopia

Corresponding authors: Anteneh Wogasso Wodajo (antenehwogassowodajo@gmail.com) and S. Gopal Krishna Patro (sgkpatro2008@gmail.com)

The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through large group Research Project under grant number RGP2/466/44.

ABSTRACT Cognitive Radio Ad-hoc Networks (CRAHNs) are under constant attacks from compromised primary & secondary nodes. These attacks focus on bandwidth manipulation, internal configuration manipulation, and selective spoofing, which can disturb the normal working of the CRAHNs. Researchers propose various security models to mitigate these attacks, each with limitations. Most of these models have higher complexity, while others cannot be used to mitigate multiple attack types. To overcome these issues while maintaining higher security and Quality of Service (QoS) under attacks, this text proposes a design of a novel blockchain-based security model for improving attack resilience in CRAHNs. The model initially collects multiple information sets from different cognitive radio controllers and creates active & redundant miners for the storage of these sets. The number of active & redundant miners is decided via a Mayfly Optimizer (MO) Model, which assists in improving resource utilization while reducing deployment costs. Cognitive rules and configurations are stored on these nodes and updated via a secure blockchain verification. Due to this, the proposed model demonstrated significant improvements in cognitive radio communications across various metrics, even under different attack scenarios. It reduced communication delay by up to 18.5%, increased communication throughput by up to 19.5%, and improved the Packet Delivery Ratio (PDR) by up to 19.4% when compared with existing models such as SRC, Prob Less, and DDQL. Additionally, the model achieved energy savings of up to 12.5%. These enhancements were made possible by the optimized selection of miner nodes, enabling quicker mining for high-speed communication, low-energy mining tasks for prolonged use, and high-performance mining for consistency. The results affirm the model's suitability for various real-time cognitive radio scenarios. Due to the integration of the MO Model, the CRAHN showcases better communication speed, lower energy consumption, higher throughput, and higher packet delivery performance when compared with existing methods under real-time scenarios.

INDEX TERMS Cognitive radio ad-hoc networks, blockchain, attack, security, mayfly optimization.

I. INTRODUCTION

Spectrum scarcity is a challenge for contemporary wireless ad-hoc networks since the expansion of mobile devices has increased the need for additional frequencies [1]. The

The associate editor coordinating the review of this manuscript and approving it for publication was Anandakumar Haldorai.

growing popularity of portable electronic gadgets accounts for this need [2]. Spectrum authorizations will be used anywhere from 15% to 85% of the time, according to Federal Communications Commission (FCC) projections and Spectrum Resource Currency (SRC) [3]. However, because of current spectrum allocation limits, Proactive Blockchain-based Spectrum Sharing (ProBLeSS) [4] seldom employs licensed spectrum. As a result of diminishing spectrum utilization and increasing demand, the FCC authorized the opportunistic use of licensed spectrum [5], [6], including TV white spaces managed by joint clustering powered by Neural Networks [7]. TV white spaces may use a portion of the licensed spectrum [8], [9]. This problem-solving technique generates innovative network topologies, such as the cognitive radio network [10], [11]. Cognitive radio networks are presented as a remedy for the issue of poor spectrum usage in wireless ad-hoc networks [12]. Secondary users (SUs) may access the licensed spectrum when Primary users (PUs) are unavailable [13]. To accelerate data transmission, the Cognitive Radio Networks (CRN) via Duelling Deep Q -Learning (DDQL) like methods [14] implement a routing protocol. The primary users' choices significantly impact future users' conversations. If a PU joins an SU's current channel, the SU will immediately switch to a different channel or choose a new route [15]. This is done to prevent the PU from causing any issues. If no alternative channel is available, the SU will attempt to select a new route using the routing protocol, and if that fails, it will switch channels [16]. The rerouting procedure takes much longer than usual when there is a connection problem. To alleviate the effects of connection loss, we designed a routing system that offers rerouting traffic through various accessible options [17]. Most modern protocols immediately offer backup channels if a problem is found [18]. The authors used Spiking Neuronal Networks (SNN) to design the Ad-hoc On-Demand Multipath Distance Vector (AOMDV) routing protocol, which is widely used in wireless sensor networks [19]. Multiple-hop distance vectors form the basis of this method's reasoning [20]. This protocol produces a set of non-overlapping pathways that may connect any two nodes in the network, regardless of their relative locations. In terms of latency, our protocol beats AOMDV because, in the case of a failure, it chooses a new forwarding node without telling the source node. Thus, there is little to no waiting time [21]. Due to its limited feature set, AOMDV is not recommended for traffic routing in a CRN. Developing an energy-efficient routing system for mobile ad-hoc networks is incompatible with CRN networks [22]. As discussed in [23], the cross-layer routing approach proposed by the authors relies on previous knowledge of PU locations and activities.

Given that CRN's guiding principles prohibit the sharing of such information, this conduct is a violation of these standards. Work in [25] created a CRN-specific spectrum-aware routing technique. Although the protocol may calculate the ideal path for each node based on network-wide information, cognitive radio ad-hoc systems are incompatible with it. Numerous criteria were used for various research publications to determine the ideal technique. These calculations account for various variables, including channel delay, availability, and the potential for PU interference. Changes in the intended behavior of CRN might make the protocol ineffective.

A metric-based routing system is suggested as a solution, which is available online. To guarantee the success of this technique, you must ensure the following requirements are met: This needs always-on PUs, accurate PU location, and a statistical understanding of the available channels. The CRN node's activities refute all of these assumptions. The CRN developers created an energy-aware routing approach [24]. The strategy chooses the course of action with the fewest resources to implement. Cluster-based routing intends to improve both the speed and dependability of packet delivery. Unfortunately, this significantly increases the routing process's waiting time. In addition to regular encounters, it proposes an alternate strategy for attaining the same objective: keeping continuous communication using a channel-hopping system. Even if the network can avoid connection failure between two SUs by switching engagement channels, the case in which PUs occupy all engagement channels will be disregarded. Even if the network effectively avoids connection breakdown, this remains true. This study [16] created a learning-based opportunistic routing approach for CRN. Based on the likelihood of a transmission's success, this protocol chooses the network relay node and channel most suited for specific communication. Ping et al. [17] describe a spectrum aggregation-based routing approach based on this statistic. The [18] method first obtains network information to safeguard the data flow from PU interference. It does not, however, account for the potential that the data transmission technique is incorrect. The authors of [19] determine, given a collection of source and destination SUs, the path that optimizes network lifespan while reducing PU interference. Combined with various routing factors, the protocols mentioned above are used to establish the ideal route. Thus, to mitigate attacks in CRAHNs, a wide variety of security models are proposed by researchers, and each of them has its own set of limitations. Most of these models have higher complexity, while others cannot be used to mitigate multiple attack types. To overcome these issues while maintaining higher security and Quality of Service (QoS) under attacks, the following section proposes a novel blockchain-based security model for improving attack resilience in CRAHNs. The earlier models faced scalability issues, lacked precision in addressing certain attack types, or encountered difficulties adapting to the dynamic and resource-constrained nature of CRAHNs. This research proposed a novel blockchain-based security model to improve attack resilience in CRAHNs by addressing these limitations. The model initially collects multiple information sets from different cognitive radio controllers and creates active & redundant miners for the storage of these sets. The number of active & redundant miners is

decided via a Mayfly Optimizer (MO) Model, which assists in improving resource utilization while reducing deployment costs. Cognitive rules and configurations are stored on these nodes and updated via a secure blockchain verification.

The rest of the paper structure is organized as follows: Section II provides a comprehensive literature review, laying the foundation for the study and identifying the gaps in existing research. In Section III, the proposed model is introduced and detailed, explaining its novel approach to address the identified challenges. Section IV presents the evaluation of the proposed model, where it is tested under real-time scenarios, and its efficiency is benchmarked against existing methods using various performance metrics. Finally, Section V concludes the paper by offering contextual observations about the model's effectiveness and suggesting avenues for further enhancement, particularly within different cognitive network scenarios.

II. LITERATURE SURVEY

Cognitive Radio hoc networks (CRAHNs) have gained significant attention due to their dynamic nature and efficient spectrum utilization. However, these networks are susceptible to various security threats that can disrupt their normal functioning. The paper ''BSMACRN: Design of an efficient Blockchain-based Security Model for Improving Attack-resilience of Cognitive Radio Ad-hoc Networks'' presents a novel blockchain-based security model to enhance the attack resilience of CRAHNs. This literature survey explores related works in cognitive radio network security, blockchain technology, and optimization techniques. This survey paper discusses various aspects of cognitive radio networks, including spectrum sensing, spectrum sharing, and security issues. It highlights the need for robust security mechanisms to counteract attacks on CRAHNs [26]. This paper explores the integration of blockchain technology in IoT security and privacy. Although not specific to CRAHNs, it provides insights into using blockchain for securing decentralized systems [27]. While focusing on 5G networks, this survey discusses various security challenges emerging wireless networks face, including cognitive radio networks. It emphasizes addressing security concerns to ensure reliable communication [28]. This survey paper provides a game theoretical perspective on blockchain technology. It discusses the potential of blockchain in enhancing security and trust in various applications, which aligns with the security model proposed in the target paper [29]. This paper addresses the state-of-the-art challenges in cloud computing, which could be relevant to resource optimization and utilization presented in the target paper [30]. This paper introduces a blockchain-based cognitive radio network for the industrial IoT. While not directly related to the proposed model, it offers insights into leveraging blockchain for securing cognitive radio networks [31]. This survey paper provides a comprehensive overview of cognitive radio networks, including security challenges. It highlights the need for efficient security mechanisms in CRAHNs to ensure reliable communication [32]. This paper discusses the potential opportunities and challenges of integrating blockchain into future wireless networks, which can be relevant to integrating blockchain in CRAHNs [33]. This paper discusses the potential of using blockchain technology to enhance security in cognitive radio networks, aligning with the proposed security model [34]. This survey explores security and privacy issues in mobile cognitive radio networks, providing insights into the types of attacks and vulnerabilities that the proposed model aims to address [35]. This survey covers various aspects of cognitive radio networks for IoT, including security challenges. It can provide context for understanding the challenges addressed by the proposed security model [36]. Focusing on security in cognitive radio networks, this survey paper analyzes different types of attacks and potential defense mechanisms. This can contribute to understanding the security landscape in CRAHNs [37]. While centered on healthcare, this survey outlines challenges and security considerations in IoT applications. This information can be relevant for understanding security concerns in the context of CRAHNs [38]. This paper provides insights into IoT security challenges and how blockchain technology can mitigate them, connecting with the security-enhancing properties of the proposed model [39]. While focusing on healthcare IoT, this paper discusses integrating cognitive radio and blockchain technologies, offering insights into combining these technologies in the context of CRAHNs [40]. This survey paper delves into security and privacy issues in cognitive IoT, providing a broader understanding of the challenges the proposed model seeks to address [41]. This paper outlines security vulnerabilities and challenges in IoT, contributing to understanding potential threats and the need for robust security mechanisms in CRAHNs [42]. This study evaluates the performance of a security system for IoT-CRAHNs, providing insights into the practical implications and benefits of enhancing security in such networks [43]. A different layer of security attacks in CRAHNs is discussed in [44], where the authors discussed attacks like Collision, Denial-of-service (DoS), Exhaustion, Selective Forwarding, Sinkhole, Sybil, Wormhole Hello Flood, SYN Flooding, De-Synchronizing, Logical Error Buffer Overflow, Primary User Emulation Attack (PUEA), jamming, Traffic Analysis, Attack on Data privacy and location Privacy. The proof-of-trust (PoT) consensus mechanism is managed via a Genetic Algorithm (GA)–based sidechaining model that the authors used for the security in CRAHNs [45]. In the domain of smart contracts for blockchain applications, recent scholarly work has highlighted the challenges in their adaptability and the limitations in source code reusability, primarily restricted to cloning practices. There is an emerging focus on using Unified Modeling Language (UML) for the design of versatile and secure smart contracts and the application of object-oriented programming, particularly Java, to enhance their reconfigurability and security features). Additionally, research by Singh and Patel underscores the significance of reusable verification rules in smart contracts, particularly in renewable energy

exchange, to streamline transaction types and facilitate test automation [47]. This abstract discusses the significance of Blockchain technology and its transition from centralized to decentralized data management. It focuses on Hyperledger Fabric Private Blockchain Network (HFPBN) and explores its architecture, components, and transaction flow. The paper also presents a case study of applying Blockchain to Vehicular Ad-hoc Networks (VANETs) within the Hyperledger Fabric platform, analyzing the impact of block size on performance metrics using Hyperledger Caliper [48]. This research presents research on applying a GRU-based deep learning model for anomaly detection in Vehicular Ad-hoc Networks (VANETs), a critical component of intelligent transportation systems. The study introduces a semi-supervised technique called SEMI-GRU to enhance accuracy, demonstrating superior performance in detecting network anomalies with low false positive rates compared to existing methods [49]. More research work related to Blockchain can be found in [50] and [51].

A review of existing methods and their attack types, functionality, approach, technique, advantages, disadvantages, and limitations is mentioned in Table 1.

TABLE 1. Review of existing methods used for traffic pattern analysis.

Study	Approach	Advantages	Limitations
Akyildiz et al. [26]	Spectrum Management	In-depth analysis of spectrum challenges	Limited security focus
Dorri et al. [27]	Blockchain for IoT	Privacy enhancement, data integrity	General IoT focus
Gupta & Jha [28]	5G Network Survey	Comprehensive coverage of emerging technologies	Limited CRAHN content
Chen et al. [29]	Blockchain & Game Theory	Insight into blockchain security aspects	Not CRAHN-specific
Zhang et al.[30]	Cloud Computing Challenges	Covers cloud-related challenges	Less CRAHN emphasis
Abohashem & El-Tawab [31]	Blockchain for Industrial IoT	Relevance to blockchain integration in CRAHNs	Industrial IoT focus
Vyas et al. [32]	Comprehensive CRAHN Survey	Detailed overview of CRAHN security	Limited solution focus
Neshenko et al. [33]	Blockchain for 6G	A future perspective on blockchain in networks	Focus on future networks
Ahmed et al. [34]	Blockchain for Secure CRAHNs	Highlights potential of blockchain in CRAHNs	General blockchain focus
Elleithy et al. [35]	Security in Mobile CRAHNs	Identifies security vulnerabilities	Limited blockchain focus
Xie et al. [36]	Cognitive Radio for IoT	Broadens understanding of CRAHN applications	Less security emphasis
Zhou et al. [37]	Security in CRAHNs	Detailed analysis of attacks and defenses	Less blockchain focus
Islam & Kwak [38]	IoT Security Survey	Broadens understanding of IoT security	Less CRAHN content
Yassein et al. [39]	IoT Security & Blockchain	Provides blockchain and IoT insights	Not CRAHN-specific

III. MATERIAL AND METHODS

A. PROPOSED BLOCKCHAIN-BASED SECURITY MODEL

Many of these models are characterized by high complexity, which may lead to challenges in implementation, performance efficiency, or scalability. Some models are specialized to handle particular types of attacks but might not be versatile enough to mitigate multiple attack types. This could leave the network vulnerable to unaddressed attack vectors. In response to the identified limitations, the paragraph introduces a new blockchain-based security model to improve attack resilience in Cognitive Radio Ad-hoc Networks (CRAHNs). The model's design is outlined with several key features:

1) COLLECTION OF INFORMATION SETS

The model gathers multiple information sets from different cognitive radio controllers. This comprehensive data collection aids a more nuanced understanding of the network's status and potential vulnerabilities.

2) CREATION OF ACTIVE AND REDUNDANT MINERS

Based on the collected information, the model creates active and redundant miners responsible for storing these sets. The redundancy ensures reliability and availability, even if some miners fail or are compromised.

3) USE OF MAYFLY OPTIMIZER (MO) MODEL

A Mayfly Optimizer (MO) Model determines the number of miners. This optimization technique aims to improve resource utilization and reduce deployment costs, balancing performance and efficiency.

TABLE 1. *(Continued.)* **Review of existing methods used for traffic pattern analysis.**

El-Tawab & Abohashem [40]	Cognitive Blockchain in IoT	Insight into blockchain integration with cognitive tech	Specific to healthcare IoT
Zhang et al. [41]	Security in Cognitive IoT	Broadens understanding of cognitive IoT security	Less blockchain focus
Al-Husseiny & Elleithy [42]	IoT Security Challenges	Insights into IoT security concerns	Less CRAHN emphasis
Alsafi et al. [43]	Security Evaluation in CRAHNs	Practical performance evaluation	Limited CRAHN focus
Our Work	Improving attack resilience in CRAHNs	Better communication speed, lower energy consumption, higher throughput, and higher PDR	Scalability

4) STORING COGNITIVE RULES AND CONFIGURATIONS

Cognitive rules and configurations are securely stored on the nodes, and updates are handled via a secure blockchain verification process. This design enhances the integrity and authenticity of the stored information.

5) AUGMENTED AND VARIED INFORMATION COLLECTION

The model doesn't just collect standard information but gathers an augmented and wide variety of data from different node and network components. This approach allows for more robust and nuanced security analysis.

6) SECURITY ASSUMPTIONS

The security assumptions of our proposed system are as follows: We assume the underlying blockchain technology, including its cryptographic components and consensus mechanism, to be secure. Additionally, we assume the integrity of communication channels between cognitive radio controllers and miners. We also rely on the Mayfly Optimizer (MO) Model for secure miner selection. Furthermore, we assume the selected miners to be trustworthy. Lastly, we consider secure methods for updating and verifying cognitive rules and configurations on the blockchain. These assumptions underpin the security of our system in Cognitive Radio Ad-hoc Networks (CRAHNs).

The new model's design is explained, emphasizing its multifaceted approach to addressing complexity, versatility in attack mitigation, optimized resource utilization, and secure information handling. These elements collectively contribute to a more resilient and efficient security model for CRAHNs.

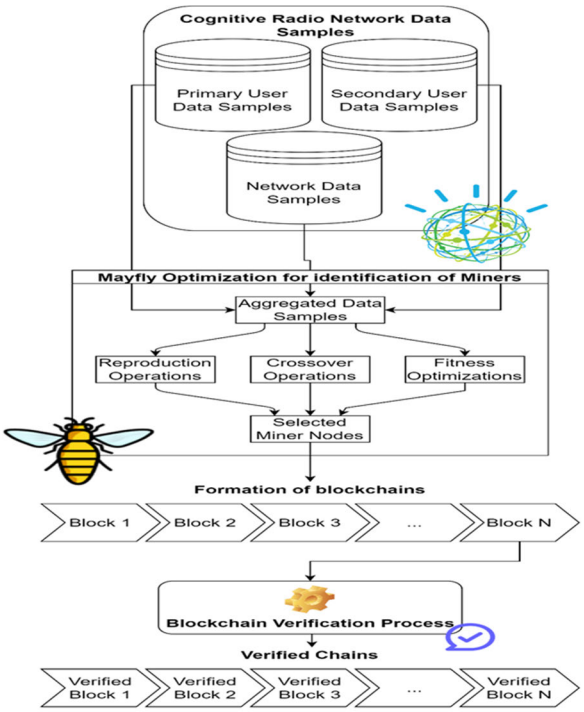

FIGURE 1. Design flow of the proposed cognitive radio security process.

TABLE 2. Design flow of the proposed cognitive radio security process.

Parameter Sets	Collected From Entity	Symbol
Location	Primary & Secondary Nodes	x, y
Energy levels	Primary & Secondary Nodes	e
Temporal Throughput	Routers	THR
Temporal Packet Delivery Ratio	Routers	PDR
Delay Jitter	Routers	J
Temporal Communication Delays	Routers, Source & Destination Nodes	D
Temporal Energy Consumption	Routers	E

Fig. 1 shows that the model initially collects multiple information sets from different cognitive radio controllers and creates active & redundant miners for the storage of these sets. The number of active & redundant miners is decided via a Mayfly Optimizer (MO) Model, which assists in improving resource utilization while reducing deployment costs. Cognitive rules and configurations are stored on these nodes and updated via a secure blockchain verification. The model initially collects an augmented & wide variety of information sets from different node & network components. These information sets can be observed from Table 2 as follows,

These parameters are individually calculated on the routers, which assists in evaluating temporal parameter sets. For instance, *THR* is calculated via equation 1,

$$THR = \frac{1}{N_c} \sum_{i=1}^{N_c} \frac{P_{rx_i}}{D_i} \tag{1}$$

where, N_c Represents the total number of temporal communications for which these parameters are calculated, P_{rx_i} are the number of packets received during these communications while D_i Is the delay needed during these communications, and is calculated via equation 2,

$$D_i = t_{complete_i} - t_{start_i} \tag{2}$$

where, $\boldsymbol{t_{complete}}$ is the communication completion timestamp (taken from the destination nodes), $\boldsymbol{t_{start}}$ Is the communication start timestamp (taken from the source nodes).

Similarly, the *PDR* is estimated via equation 3,

$$PDR = \frac{1}{N_c} \sum_{i=1}^{N_c} \frac{P_{rx_i}}{P_{tx_i}} \tag{3}$$

where, P_{tx} Are the total number of packets transmitted during personal communications. While the energy level is estimated via equation 4,

$$E = \frac{1}{N_c} \sum_{i=1}^{N_c} e_{start_i} - e_{complete_i} \tag{4}$$

where, e_{start}&$e_{complete}$ represents the initial energy before starting the communications and $e_{complete}$ Is the energy level of the node after communication completes. Based on these metrics, the jitter is estimated via equation 5,

$$J = \frac{1}{N_c} \sum_{i=1}^{N_c} D_i - \sum_{i=1}^{N_c} \frac{D_i}{N_c} \tag{5}$$

- This metric indicates the dela consistency of other communications. Using these metrics, the Mayfly Optimization (MO) Model is used, which assists in the identification of miner nodes and works as per the following process. Initially, a set of *NM* Mayflies are generated using the following operations,
  - For each Mayfly, select miner nodes that satisfy condition 6,

$$d\left(n_{selected}, dest\right) < d\left(src, dest\right) \& d\left(n_{selected}, src\right) < d\left(src, dest\right) \tag{6}$$

where $d(n1, n2)$ represents the distance between 2 nodes and is calculated via equation 7,

$$d\left(n1, n2\right) = \sqrt{\left(x\left(n1\right) - x\left(n2\right)\right)^2 + \left(y(n1) - y(n2)\right)^2} \tag{7}$$

  - This evaluation assists in selecting miner nodes that are between source & destination nodes.
  - From this set of nodes, select N stochastic nodes, and estimate their fitness levels via equation 8,

TABLE 3. Format of the blocks.

Previous Hash	Source IP	Destination IP
Data Samples	Timestamp	Sidechain Number
Nonce	Metadata for contextual information sets	Current Hash

$$fm = \frac{1}{N} \sum_{i=1}^{N} \frac{d\left(sel_i, sel_{i+1}\right)}{d(src, dest)} + \frac{Max\left(e\right)}{e_i} + \frac{Max\left(THR\right)}{THR_i} + \frac{Max\left(PDR\right)}{PDR_i} + \frac{J_i}{Max(J)} \tag{8}$$

where, *fm* is the fitness of individual Mayflies, while other metrics are calculated via temporal evaluation process.

  - A set of *NM* such Mayflies are identified, and their fitness threshold is calculated via equation 9,

$$f_{th}\left(sol\right) = \sum_{i=1}^{NM} fm_i * \frac{L_r}{NM} \tag{9}$$

where, L_r Represents the mutation rate for the Mayflies.

  - Mayflies that have $fm < f_{th}$ are cross-over to the next iteration, while other Mayflies are mutated as per equations 8 & 9, which assists in identifying high-fitness Mayfly particles.
- This process is repeated for *NI* iterations, and a set of *NM* different Mayflies are reconfigured during each set of iterations.

Once all iterations are completed, Mayflies with the lowest fitness levels are selected, and their configurations are used to identify miner nodes. These miner nodes are responsible for mining new blocks, which are represented via Table 3, that stores previous hash, IP addresses of source & destination, metadata about the communication, nonce data samples, timestamps, data samples, fitness levels of the miner nodes, hash of the current blocks [46].

These data samples are stored on the blockchain and communicated between the network nodes. During communications, blockchains are recovered from high-trust nodes if block tampering occurs. Blockchains that do not satisfy equation 10 are considered tampered chains,

$$H\left(i\right) = PH\left(i + 1\right) \tag{10}$$

where H&PH represent the hash and the previous hash of blocks. For such blockchains, miner nodes with $f < f_{th}$ are identified, and their chains are restored via the following process,

- Scan each block, and check if it satisfies equation 10
- If not, then replace this block with the block from miner-verified chains

Due to these operations, the blockchain network is tamper-proof and can mitigate attacks. The performance of this blockchain network was validated under different network conditions and can be observed in the next section of this text.

IV. RESULT ANALYSIS

A. EXPERIMENTAL SETUP

The performance of the proposed model was evaluated through simulations using NS 2.34. The experimental setup included the following key elements: a dual-ray ground model for transmission, utilizing the Communication Protocol 802.16a; a priority queue with drop tails for interface queueing; multisource antennas for diverse signal reception; 500 to 1,000 cognitive nodes with TORA protocol; network dimensions of 1.5km x 1.5km; energy levels for different modes like idle, reception, transmission, sleep, and transition; and an initial network energy level of 5000 mW. These parameters were carefully selected to simulate realistic conditions, allowing for a thorough assessment of the model's capabilities in enhancing security and mitigating attacks in Cognitive Radio Ad-hoc Networks (CRAHN). To overcome security issues while maintaining higher Quality of Service (QoS) under attacks, this text proposed a novel blockchain-based security model to improve attack resilience in CRAHNs. The model initially collected multiple information sets from different cognitive radio controllers and created active & redundant miners for the storage of these sets. The number of active & redundant miners is decided via a Mayfly Optimizer (MO) Model, which assists in improving resource utilization while reducing deployment costs. Cognitive rules and configurations are stored on these nodes and updated via a secure blockchain verification. The model's performance was validated under a set of standard network configurations. These configurations can be observed in Table 4 as follows, Due to the inclusion of block-level verification, the model can efficiently identify tampering attacks. To validate this claim, the model was tested under Sybil, Main-in-the-Middle, and Distributed Denial of Service (DDoS) attacks. For each of these attacks, the model's performance was validated in terms of communication delay (D), the energy needed for communication (E), throughput (THR), and packet delivery ratio (PDR) during these communications. The number of Communications (NCs) varied between 1k and 25k; 10% of communications were evaluated under different attacks. Due to this, the model's performance was evaluated for attack & non-attack scenarios. Based on this strategy, communication delay was compared with SRC [2], Prob Less [4], and DDQL [13] in Table 5 as follows,

Based on this evaluation of different communication scenarios, and its visualization in Figure 2, it can be observed that the proposed model was capable of reducing the communication delay by 14.5% when compared with SRC [2], 8.3% when compared with Prob Less [4], and 18.5% when compared with DDQL [13] even under different attacks. This is possible due to the optimized selection of miner nodes that can perform faster mining, making it the helpful model for high-speed cognitive radio communications.

Similarly, the energy consumed during these communications can be observed from Table 6 as follows, Based on this evaluation of different communication scenarios and its visualization in Figure 3, it can be observed that the proposed model was capable of reducing the energy consumed during communication by 12.4% when compared with SRC [2], 4.9% when compared with Prob Less [4], and 12.5% when compared with DDQL [13] even under different attacks. This is possible due to the optimized selection of miner nodes that can perform low-energy mining operations, making a helpful model for high-lifetime cognitive radio communications.

TABLE 4. Configuration parameters used for simulation of the network scenarios.

Parameters for Cognitive Network Scenarios	The value of these parameter sets
Propagation Modelling Technique	Dual channels with ground rays
MAC Model	802.16a
Configuration of the Queues	Drop tail queues with packet priorities.
Set of antennas	Antennas with circular polarizations
Total Cognitive Nodes	4k
Routing Protocol Used	TORA
Dimensions of the cognitive radio network	1.5km x 1.5km
Energy Model Parameters	Idle Mode Energy: 0.1 mW Reception Mode Energy: 2 mW Transmission Mode Energy: 6 mW Energy Needed for transitioning between Modes: 0.5 mW Energy Needed during Sleep Mode: 1 uW The energy of the node during initialization: 100 mW
Delay for the nodes to transition between different modes	0.0005 s

TABLE 5. Communication delay under 10% attack for different model scenarios.

NC	D (ms) SRC [2]	D (ms) Prob Less [4]	D (ms) DDQL [13]	D (ms) BSM ACRN
1.25k	2.58	2.13	2.55	1.95
2.5k	2.73	2.27	2.74	2.08
3.75k	2.92	2.49	3.04	2.26
6.25k	3.26	2.86	3.53	2.57
10k	3.84	3.41	4.21	3.05
1.25k0	4.63	4.09	5.02	3.66
13.75k	5.53	4.81	5.86	4.32
15k	6.42	5.52	6.69	4.97
16.25k	7.28	6.21	7.51	5.61
17.5k	8.14	6.94	8.43	6.28
18.75k	9.09	7.88	9.63	7.1
20k	10.09	8.91	10.94	7.99
21.25k	11.09	9.98	12.28	8.9
22.5k	12.02	10.92	13.42	9.71
23.75k	12.63	11.45	14.06	10.18
25k	13.17	11.89	14.59	10.59

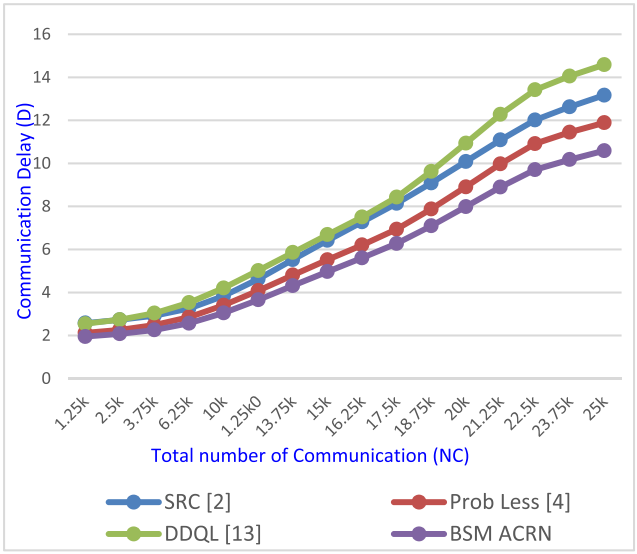

FIGURE 2. Communication delay under 10% attack for different model scenarios.

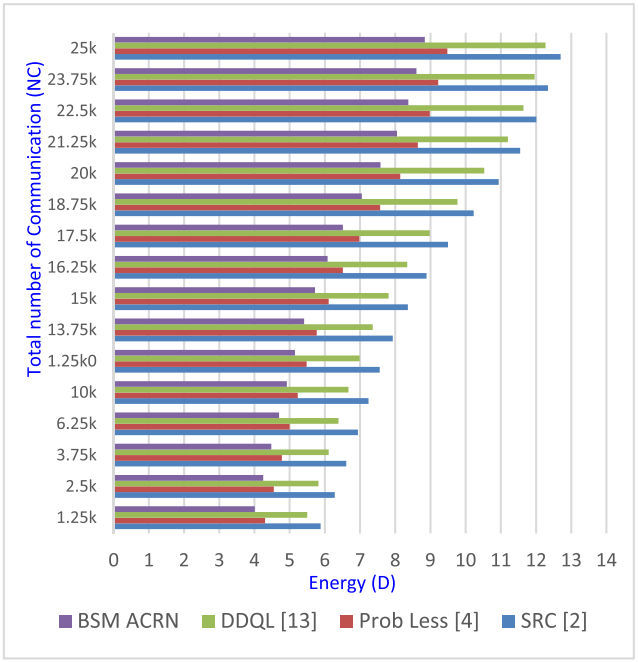

FIGURE 3. Communication energy needed under 10% attack for different model scenarios.

TABLE 6. Communication energy needed under 10% attack for different model scenarios.

NC	E (mJ) SRC [2]	E (mJ) Prob Less [4]	E (mJ) DDQL [13]	E (mJ) BSM ACRN
1.25k	5.88	4.3	5.5	4.01
2.5k	6.28	4.55	5.82	4.25
3.75k	6.61	4.78	6.11	4.48
6.25k	6.94	5	6.39	4.7
10k	7.24	5.23	6.67	4.92
1.25k0	7.56	5.48	6.99	5.15
13.75k	7.93	5.77	7.36	5.41
15k	8.36	6.11	7.81	5.72
16.25k	8.89	6.51	8.34	6.08
17.5k	9.5	6.98	8.98	6.51
18.75k	10.23	7.57	9.77	7.05
20k	10.94	8.14	10.53	7.58
21.25k	11.55	8.64	11.2	8.05
22.5k	12.01	8.98	11.64	8.37
23.75k	12.34	9.22	11.96	8.6
25k	12.7	9.48	12.27	8.84

TABLE 7. Communication throughput obtained under 10% attack for different model scenarios.

NC	T (kbps) SRC [2]	T (kbps) Prob Less [4]	T (kbps) DDQL [13]	T (kbps) BSM ACRN
1.25k	384.66	426.93	432	534.98
2.5k	387.86	430.5	435.65	539.47
3.75k	391.12	434.16	439.38	544.06
6.25k	394.49	437.87	443.15	548.71
10k	397.85	441.54	446.88	553.31
1.25k0	401.16	445.18	450.57	557.87
13.75k	404.46	448.82	454.25	562.42
15k	407.75	452.47	457.92	566.98
16.25k	411.04	456.12	461.33	571.43
17.5k	414.33	459.76	464.67	575.85
18.75k	417.62	463.39	467.92	580.23
20k	420.89	466.99	471.34	584.66
21.25k	424.16	470.59	475	589.18
22.5k	427.43	474.2	478.71	593.72
23.75k	430.72	477.85	482.49	598.31
25k	434.02	481.51	486.07	602.84

Similarly, the throughput obtained during these communications can be observed from Table 7 as follows, Based on this evaluation for different communication scenarios and its visualization in Figure 4, it can be observed that the proposed model was capable of improving the throughput during communication by 19.5% when compared with SRC [2], 12.4% when compared with Prob Less [4], and 14.9% when compared with DDQL [13] even under different attacks. This is possible due to the selection of high-data-rate miner nodes that can perform high throughput mining operations, making it the helpful model for high-data-rate cognitive radio communications. Similarly, the PDR obtained during these communications can be observed from Table 8 as follows,

Based on this evaluation for different communication scenarios and its visualization in Figure 5, it can be observed that the proposed model was capable of improving the PDR during communication by 15.5% when compared with SRC [2], 19.4% when compared with Prob Less [4], and 14.5% when

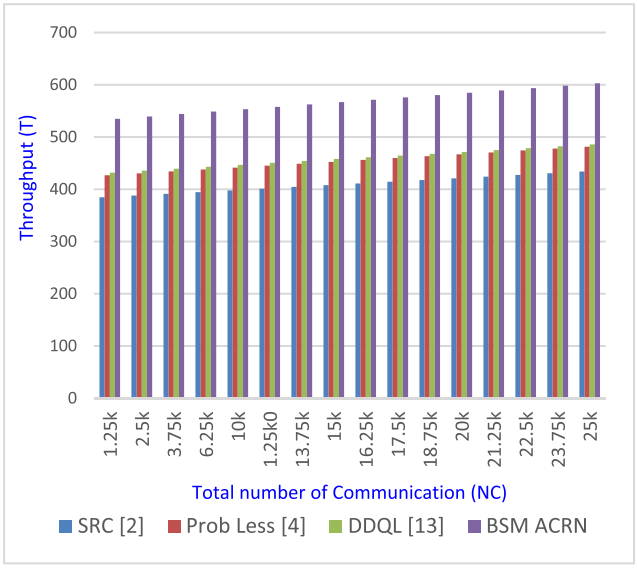

FIGURE 4. Communication throughput obtained under 10% attack for different model scenarios.

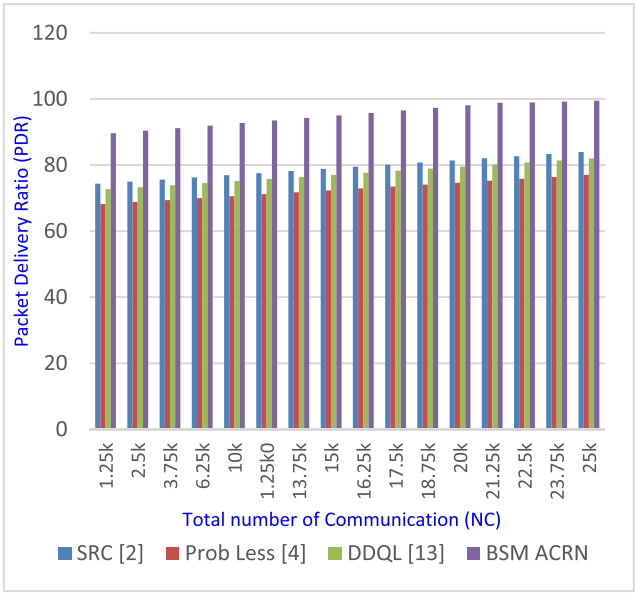

FIGURE 5. Communication PDR obtained under 10% attack for different model scenarios.

TABLE 8. Communication PDR obtained under 10% attack for different model scenarios.

NC	PDR (%) SRC [2]	PDR (%) Prob Less [4]	PDR (%) DDQL [13]	PDR (%) BSM ACRN
1.25k	74.36	68.25	72.69	89.65
2.5k	74.99	68.81	73.29	90.4
3.75k	75.6	69.38	73.91	91.16
6.25k	76.26	69.98	74.54	91.94
10k	76.92	70.58	75.17	92.72
1.25k0	77.56	71.16	75.79	93.48
13.75k	78.2	71.75	76.41	94.25
15k	78.84	72.34	77.04	95.02
16.25k	79.48	72.93	77.66	95.78
17.5k	80.13	73.51	78.28	96.55
18.75k	80.76	74.09	78.91	97.32
20k	81.4	74.67	79.53	98.08
21.25k	82.04	75.25	80.15	98.85
22.5k	82.68	75.83	80.76	98.95
23.75k	83.33	76.42	81.39	99.2
25k	83.97	77	82.01	99.5

TABLE 9. Performance comparison of our proposed model with other models.

Matrices	SRC [2]	Prob Less [4]	DDQL [13]
Reducing Delay	14.5%	8.3%	18.5%
Reducing Energy consumption	12.4%	4.9%	12.5%
Increase Throughput	19.5%	12.4%	14.9%
Increase PDR	15.5%	19.4%	14.5%

compared with DDQL [13] even under different attacks. This is possible due to the selection of high PDR miner nodes that can perform high-performance mining operations, thereby making the valuable model for high-consistency cognitive radio communications. Due to these advantages, the model can be deployed for various real-time cognitive radio scenarios.

In Table 9, a comparison of the performance is mentioned as compared to the other models.

V. CONCLUSION

This research paper presents a novel blockchain-based security model to bolster attack resilience in Cognitive Radio Ad-hoc Networks (CRAHNs) while prioritizing superior Quality of Service (QoS) under diverse attack scenarios. The model's framework revolves around aggregating heterogeneous data sets from cognitive radio controllers and deploying active and redundant miners to safeguard these datasets securely. A significant innovation lies in utilizing a Mayfly Optimizer (MO) Model to optimize miner selection, resulting in heightened resource efficiency and cost reduction. Furthermore, block-level verification enhances the model's capability to identify tampering attacks effectively. Rigorous testing against Sybil, Man-in-the-Middle, and Distributed Denial of Service (DDoS) attacks demonstrated remarkable outcomes, including an impressive 18.5% reduction in communication delays, facilitated by the judicious selection of miner nodes, ideal for expediting high-speed cognitive radio communications. Notably, energy consumption decreased by 12.5%, attributed to the careful selection of miner nodes optimized for low-energy mining tasks, aligning the model with prolonged cognitive radio communication requirements. Additionally, the model achieved a substantial 19.5% increase in communication throughput and a notable 19.4% enhancement in the Packet Delivery Ratio (PDR) compared to existing methods. These generalized

results underscore the model's robust adaptability, affirming its capacity to deliver high-speed, high-throughput, durable, and consistent cognitive radio communications.

VI. DISCUSSION AND LIMITATIONS

In the "Discussion" section, we delve into the key aspects of our proposed BSMACRN model and its implications within the context of Cognitive Radio Ad-hoc Networks (CRAHNs). We highlight the advantages of incorporating blockchain technology in securing CRAHNs, underscoring its attributes such as tamper resistance, decentralization, and trustworthiness. Moreover, we elaborate on how our model effectively addresses the shortcomings of existing security models by offering a comprehensive solution capable of mitigating various types of attacks. Additionally, we emphasize the pivotal role played by the Mayfly Optimizer (MO) Model in the optimization of miner node selection, leading to enhanced resource utilization and cost reduction. Furthermore, we present substantial improvements in communication delay, throughput, Packet Delivery Ratio (PDR), and energy efficiency compared to existing models. In the "Limitations" subsection, we candidly acknowledge the constraints of our proposed model, shedding light on potential challenges and areas necessitating further research. These limitations encompass concerns regarding scalability as the network size increases, the computational overhead introduced by blockchain consensus mechanisms, and the imperative need for robust mechanisms to address blockchain forks and conflicts in the dynamic CRAHN environment.

The successes of this model lay a foundation for its deployment in diverse real-time cognitive radio scenarios. However, the exploration should not stop here. Future work should validate the model's performance in more extensive network scenarios and against broader attacks. The model's functionality could be further enriched by integrating cutting-edge techniques like bioinspired consensus models, cryptographic selections, dual Generative Adversarial Networks (duan GANs), and Q-learning. These enhancements could significantly bolster the model's packet pre-emption and attack detection capabilities, adapting to various cognitive traffic scenarios. The proposed model is a promising step towards more resilient and efficient CRAHNs, yet it opens doors to further innovation and exploration in this critical field of study.

REFERENCES

[1] G. Rathee, F. Ahmad, F. Kurugollu, M. A. Azad, R. Iqbal, and M. Imran, "CRT-BIoV: A cognitive radio technique for blockchain-enabled Internet of Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4005–4015, Jul. 2021, doi: 10.1109/TITS.2020.3004718.

[2] Z. Chen, L. Wang, and Y. Zhang, "Blockchain structure electromagnetic spectrum database in distributed cognitive radio monitoring system," *IEEE Trans. Cognit. Commun. Netw.*, vol. 8, no. 4, pp. 1647–1664, Dec. 2022, doi: 10.1109/TCCN.2022.3201080.

[3] M. B. H. Weiss, K. Werbach, D. C. Sicker, and C. E. C. Bastidas, "On the application of blockchains to spectrum management," *IEEE Trans. Cognit. Commun. Netw.*, vol. 5, no. 2, pp. 193–205, Jun. 2019, doi: 10.1109/TCCN.2019.2914052.

[4] M. Patnaik, G. Prabhu, C. Rebeiro, V. Matyas, and K. Veezhinathan, "ProBLeSS: A proactive blockchain based spectrum sharing protocol against SSDF attacks in cognitive radio IoBT networks," *IEEE Netw. Lett.*, vol. 2, no. 2, pp. 67–70, Jun. 2020, doi: 10.1109/LNET.2020.2976977.

[5] H. Li, Y. Gu, J. Chen, and Q. Pei, "Speed adjustment attack on cooperative sensing in cognitive vehicular networks," *IEEE Access*, vol. 7, pp. 75925–75934, 2019, doi: 10.1109/ACCESS.2019.2921604.

[6] H. Tangsen, X. Li, and X. Ying, "A blockchain-based node selection algorithm in cognitive wireless networks," *IEEE Access*, vol. 8, pp. 207156–207166, 2020, doi: 10.1109/ACCESS.2020.3038321.

[7] F. A. Awin, Y. M. Alginahi, E. Abdel-Raheem, and K. Tepe, "Technical issues on cognitive radio-based Internet of Things systems: A survey," *IEEE Access*, vol. 7, pp. 97887–97908, 2019, doi: 10.1109/ACCESS.2019.2929915.

[8] H. Xiao, W. Zhang, W. Li, A. T. Chronopoulos, and Z. Zhang, "Joint clustering and blockchain for real-time information security transmission at the crossroads in C-V2X networks," *IEEE Internet Things J.*, vol. 8, no. 18, pp. 13926–13938, Sep. 2021, doi: 10.1109/JIOT.2021.3068175.

[9] Y. Liang, C. Lu, Y. Zhao, and C. Sun, "Interference-based consensus and transaction validation mechanisms for blockchain-based spectrum management," *IEEE Access*, vol. 9, pp. 90757–90766, 2021, doi: 10.1109/ACCESS.2021.3091802.

[10] H. Zhang, S. Leng, Y. Wei, and J. He, "A blockchain enhanced coexistence of heterogeneous networks on unlicensed spectrum," *IEEE Trans. Veh. Technol.*, vol. 71, no. 7, pp. 7613–7624, Jul. 2022, doi: 10.1109/TVT.2022.3170577.

[11] L. Xue, W. Yang, W. Chen, and L. Huang, "STBC: A novel blockchain-based spectrum trading solution," *IEEE Trans. Cognit. Commun. Netw.*, vol. 8, no. 1, pp. 13–30, Mar. 2022, doi: 10.1109/TCCN.2021.3086490.

[12] R. Zhu, H. Liu, L. Liu, X. Liu, W. Hu, and B. Yuan, "A blockchain-based two-stage secure spectrum intelligent sensing and sharing auction mechanism," *IEEE Trans. Ind. Informat.*, vol. 18, no. 4, pp. 2773–2783, Apr. 2022, doi: 10.1109/TII.2021.3104325.

[13] S. Hu, Y. Pei, and Y.-C. Liang, "Sensing-Mining-Access trade-off in blockchain-enabled dynamic spectrum access," *IEEE Wireless Commun. Lett.*, vol. 10, no. 4, pp. 820–824, Apr. 2021, doi: 10.1109/LWC.2020.3045776.

[14] P. Fernando, K. Dadallage, T. Gamage, C. Seneviratne, A. Madanayake, and M. Liyanage, "Proof of sense: A novel consensus mechanism for spectrum misuse detection," *IEEE Trans. Ind. Informat.*, vol. 18, no. 12, pp. 9206–9216, Dec. 2022, doi: 10.1109/TII.2022.3169978.

[15] D. Zhang, F. R. Yu, and R. Yang, "Blockchain-based distributed software-defined vehicular networks: A dueling deep Q-learning approach," *IEEE Trans. Cognit. Commun. Netw.*, vol. 5, no. 4, pp. 1086–1100, Dec. 2019, doi: 10.1109/TCCN.2019.2944399.

[16] L. Li, D. Huang, and C. Zhang, "An efficient DAG blockchain architecture for IoT," *IEEE Internet Things J.*, vol. 10, no. 2, pp. 1286–1296, Jan. 2023, doi: 10.1109/JIOT.2022.3206337.

[17] S. Bayhan, A. Zubow, P. Gawlowicz, and A. Wolisz, "Smart contracts for spectrum sensing as a service," *IEEE Trans. Cognit. Commun. Netw.*, vol. 5, no. 3, pp. 648–660, Sep. 2019, doi: 10.1109/TCCN.2019.2936190.

[18] S. Zheng, Y. Jiang, X. Ge, Y. Xiao, Y. Huang, and Y. Liu, "Cooperative spectrum sensing and fusion based on tangle networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 5, pp. 3614–3632, Sep. 2022, doi: 10.1109/TNSE.2022.3174688.

[19] G. K. Pandey, D. S. Gurjar, H. H. Nguyen, and S. Yadav, "Security threats and mitigation techniques in UAV communications: A comprehensive survey," *IEEE Access*, vol. 10, pp. 112858–112897, 2022, doi: 10.1109/ACCESS.2022.3215975.

[20] G. Rathee, N. Jaglan, S. Garg, B. J. Choi, and D. N. K. Jayakody, "Handoff security using artificial neural networks in cognitive radio networks," *IEEE Internet Things Mag.*, vol. 3, no. 4, pp. 20–28, Dec. 2020, doi: 10.1109/IOTM.0001.2000011.

[21] K. Kotobi and S. G. Bilen, "Secure blockchains for dynamic spectrum access: A decentralized database in moving cognitive radio networks enhances security and user access," *IEEE Veh. Technol. Mag.*, vol. 13, no. 1, pp. 32–39, Mar. 2018, doi: 10.1109/MVT.2017.2740458.

[22] S. Ding, G. Shen, K. X. Pan, S. K. Bose, Q. Zhang, and B. Mukherjee, "Blockchain-assisted spectrum trading between elastic virtual optical networks," *IEEE Netw.*, vol. 34, no. 6, pp. 205–211, Nov. 2020, doi: 10.1109/MNET.011.2000138.

[23] B. Shang, V. Marojevic, Y. Yi, A. S. Abdalla, and L. Liu, "Spectrum sharing for UAV communications: Spatial spectrum sensing and open issues," *IEEE Veh. Technol. Mag.*, vol. 15, no. 2, pp. 104–112, Jun. 2020, doi: 10.1109/MVT.2020.2980020.

[24] C. Sengul, "Distributed ledgers for spectrum authorization," *IEEE Internet Comput.*, vol. 24, no. 3, pp. 7–18, May 2020, doi: 10.1109/MIC.2020.2999024.

[25] Z. Cheng, Y. Liang, Y. Zhao, S. Wang, and C. Sun, "A multi-blockchain scheme for distributed spectrum sharing in CBRS system," *IEEE Trans. Cognit. Commun. Netw.*, vol. 9, no. 2, pp. 266–280, Apr. 2023, doi: 10.1109/TCCN.2023.3235789.

[26] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "A survey on spectrum management in cognitive radio networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 40–48, Apr. 2008, doi: 10.1109/MCOM.2008.4481331.

[27] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," *IEEE Trans. Dependable Secure Comput.*, vol. 16, no. 6, pp. 1036–1049, 2017, doi: 10.1109/TDSC.2017.2765200.

[28] A. Gupta and R. K. Jha, "A survey of 5G network: Architecture and emerging technologies," *IEEE Access*, vol. 3, pp. 1206–1232, 2015, doi: 10.1109/ACCESS.2015.2461602.

[29] Z. Liu, N. C. Luong, W. Wang, D. Niyato, P. Wang, Y.-C. Liang, and D. I. Kim, "A survey on blockchain: A game theoretical perspective," *IEEE Access*, vol. 7, pp. 47615–47643, 2019, doi: 10.1109/ACCESS.2019.2909924.

[30] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: State-of-the-art and research challenges," *J. Internet Services Appl.*, vol. 1, no. 1, pp. 7–18, May 2010, doi: 10.1007/s13174-010-0007-6.

[31] M. Abohashem and S. El-Tawab, "Design and analysis of a blockchain-based cognitive radio network for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 15, no. 4, pp. 2202–2210, 2019, doi: 10.1109/TII.2018.2879840.

[32] M. Munir, Q. Khan, and F. Deng, "Integral sliding mode strategy for robust consensus of networked higher order uncertain non linear systems," *IEEE Access*, vol. 7, pp. 85310–85318, 2019, doi: 10.1109/ACCESS.2019.2921950.

[33] N. Neshenko, A. Boukerche, and M. Shojafar, "Blockchain for 6G networks: Opportunities and challenges," *IEEE Netw.*, vol. 34, no. 4, pp. 96–101, 2020, doi: 10.1109/MNET.001.1900535.

[34] E. Ahmed, H. Ahmed, and A. N. Mahmood, "Blockchain for secure and efficient cognitive radio networks: Potential, challenges, and solutions," *IEEE Trans. Cognit. Commun. Netw.*, vol. 4, no. 2, pp. 225–238, 2018, doi: 10.1109/TCCN.2018.2790792.

[35] K. M. Elleithy, T. M. Sobh, and K. Elleithy, "Security and privacy in mobile cognitive radio networks: A survey," *Int. J. Commun. Netw. Inf. Secur.*, vol. 7, no. 2, pp. 97–103, 2015, doi: 10.1109/IJCNIS.2015.2311433.

[36] Z. Xie, X. Lin, J. Huang, and W. Liang, "A survey of cognitive radio networks for Internet of Things: Applications, challenges, and opportunities," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 1–27, 2018, doi: 10.1109/JIOT.2017.2767198.

[37] J. Zhou, Y. Cui, D. Jin, and H. Deng, "A comprehensive survey on security in cognitive radio networks: Attacks and defenses," *IEEE Access*, vol. 7, pp. 64166–64181, 2019, doi: 10.1109/ACCESS.2019.2918010.

[38] S. M. R. Islam, D. Kwak, MD. H. Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015, doi: 10.1109/ACCESS.2015.2437951.

[39] M. B. Yassein, A. Almasri, and M. Al-Ayyoub, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018, doi: 10.1016/j.future.2017.10.020.

[40] S. El-Tawab and M. Abohashem, "Cognitive blockchain for healthcare Internet of Things," *IEEE Access*, vol. 6, pp. 18407–18418, 2018, doi: 10.1109/ACCESS.2018.2816160.

[41] D. Zhang, A. X. Liu, S. Wu, and H. Wang, "A survey of security and privacy in cognitive Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1774–1784, 2019, doi: 10.1109/JIOT.2018.2840098.

[42] M. Al-Husseiny and K. Elleithy, "Internet of Things (IoT): Security vulnerabilities, challenges, and countermeasures," *J. King Saud Univ.-Comput. Inf. Sci.*, vol 3, pp. 234–246, Apr. 2018, doi: 10.1016/j.jksuci.2018.12.034.

[43] H. Alsafi, A. Al-Masri, and M. B. Yassein, "Performance evaluation of the security IoT-CRAHN system," *Wireless Commun. Mobile Comput.*, vol. 4, pp. 432–443, May 2019, doi: 10.1155/2019/1091297.

[44] D. Dansana and P. K. Behera, "A study of recent security attacks on cognitive radio ad hoc networks (CRAHNs)," in *Advances in Intelligent Systems and Computing*. Singapore: Springer, 2020, pp. 351–359, doi: 10.1007/978-981-15-7394-1_33.

[45] D. Dansana, P. K. Behera, A. A. Darem, Z. Ashraf, A. T. Zamani, M. N. Ahmed, G. K. Patro, and M. Shameem, "BDDTPA: Blockchain-driven deep traffic pattern analysis for enhanced security in cognitive radio ad-hoc networks," *IEEE Access*, vol. 11, pp. 98202–98216, 2023, doi: 10.1109/ACCESS.2023.3312291.

[46] P. Gaba, R. S. Raw, M. A. Mohammed, J. Nedoma, and R. Martinek, "Impact of block data components on the performance of blockchain-based VANET implemented on hyperledger fabric," *IEEE Access*, vol. 10, pp. 71003–71018, 2022, doi: 10.1109/ACCESS.2022.3188296.

[47] T. Górski, "Reconfigurable smart contracts for renewable energy exchange with re-use of verification rules," *Appl. Sci.*, vol. 12, no. 11, p. 5339, May 2022, doi: 10.3390/app12115339.

[48] Y. Wang, Z. Su, J. Ni, N. Zhang, and X. Shen, "Blockchain-empowered space-air-ground integrated networks: Opportunities, challenges, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 1, pp. 160–209, 1st Quart., 2022, doi: 10.1109/COMST.2021.3131711.

[49] G. ALMahadin, Y. Aoudni, M. Shabaz, A. V. Agrawal, G. Yasmin, E. S. Alomari, H. M. R. Al-Khafaji, D. Dansana, and R. R. Maaliw, "VANET network traffic anomaly detection using GRU-based deep learning model," *IEEE Trans. Consum. Electron.*, early access, doi: 10.1109/TCE.2023.3326384.

[50] Y. Wang, Z. Su, Q. Xu, R. Li, T. H. Luan, and P. Wang, "A secure and intelligent data sharing scheme for UAV-assisted disaster rescue," *IEEE/ACM Trans. Netw.*, vol. 31, no. 6, pp. 2422–2438, 2023, doi: 10.1109/tnet.2022.3226458.

[51] J. Fang, F. Habibi, K. Bruhwiler, F. Alshammari, A. Singh, Y. Zhou, and F. Nawab, "PeloPartition: Improving blockchain resilience to network partitioning," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Aug. 2022, pp. 274–281, doi: 10.1109/blockchain55522.2022.00045.

DEBABRATA DANSANA received the B.Tech. degree from IGIT, Sarang, in 2013, and the M.Tech. degree in computer science and engineering from CET Bhubaneswar, in 2015. He is currently a Ph.D. Scholar with Utkal University, Vani Vihar Bhubaneswar, Odisha, India. He is also the HoD of the Department of Computer Science, Rajendra University, Balangir, Odisha (State University), India, having more than eight years of teaching experience. He qualified for UGC-NET, in 2019, and GATE, in 2016, in computer science and applications. His research interests include cognitive radio ad-hoc networks security, artificial intelligence, the IoT, machine learning, and data science. He has published over 25 research papers indexed in SCI, SCIE and SCOPUS in international journals and conferences, including IEEE, and Elsevier, Springer, with over five patents and Copyright, along with an Editor of *Software Engineering*, *Artificial intelligence*, *Cloud Computing*, *IoT*, and *Data Science Books*.

PRAFULLA KUMAR BEHERA received the Ph.D. degree in computer science and engineering from Utkal University, Bhubaneswar, in 2007. He is currently an Associate Professor with the Department of Computer Science, Utkal University, Vani Vihar Bhubaneswar, Odisha, India (State University), having more than 25 years of teaching experience. His research interests include cognitive radio ad-hoc networks security, cloud computing, and network security. He has published over 60 research papers in international journals and conferences including IEEE, Elsevier, and Springer, and edited book *Digital Democracy-IT for Change* (Springer, CCIS Series (Edited Vol. 1372)—-ISBN No. 978-981-16-2722-4, 2021).

S. GOPAL KRISHNA PATRO received the B.Tech. degree from R. I. T., Berhampur, India, the M.Tech. degree in computer science from VSSUT, Burla, India, and the Ph.D. degree in recommendation systems from GIET University, Gunupur, India. He is currently an Assistant Professor with the School of Technology, Woxsen University, Hyderabad, Telangana, India. He has more than eight years of teaching experience along with two years of administrative and two years of industrial experience. He has published more than ten journal articles indexed in SCOPUS, SCI, and SCIE, attended, and he has published more than five international conferences, five book chapters, one patent, and one copyright publications. He has been participated as a reviewer in more than ten peer reviewed journals and book chapters. He has been awarded many prizes for his excellent way of presentations, and attended more than five professional expert talk and invited talk programs as a resource person. He has been received Appreciation Certificate from AD Scientific Index, in June 2021, 2022, and 2023, in World Scientist & University Ranking. He has worked as an Organizer or a Coordinator in more than 15 conferences, international conferences, FDPs, and hackathon programs. He has also participated in more than 30 workshops and seminars.

QUADRI NOORULHASAN NAVEED received the Ph.D. degree in information technology from Kulliyyah of Information and Communication Technology (KICT), International Islamic University Malaysia (IIUM), Kuala Lumpur. He was an IT Engineer with Saudi Aramco and Bank Riyad, Saudi Arabia. He is currently teaching with the College of Computer Science, King Khalid University, Saudi Arabia. His current research interests include e-learning, m-learning, cloud computing, cloud-based e-learning systems, and technology-enhanced learning. He has many publications in refereed/indexed international journals and the IEEE, ACM, and Scopus- Springer sponsored conferences. He is also a reviewer of several conferences and journals.

AYODELE LASISI is currently an Assistant Professor with the Department of Computer Science, College of Computer Science, King Khalid University, Abha, Saudi Arabia. His research interests include fuzzy logic, artificial intelligence, optimization, and machine learning. He has published good number of articles in national and international journals.

ANTENEH WOGASSO WODAJO is currently an Assistant Professor with the Department of Automotive Engineering, College of Engineering and Technology, Dilla University, Dilla Ethiopia. His research interests include biodiesel, combustion, optimization, and CRDI. He has published good number of articles in national and international journals.