Blockchain-enabled Secure Data Communication Protocols for 5G Networks

Mohanad Sameer Jabar
Technical College of Engineering, Al-Bayan University, Baghdad, Iraq
mohanad.s@albayan.edu.iq (corresponding author)

Received: 14 November 2024 | Revised: 5 December 2024 | Accepted: 22 December 2024

 DOI: https://doi.org/10.48084/etasr.9617

ABSTRACT

With the further expansion of 5G networks, a main priority continues to shift towards secure and efficient protocols for data transmission. Traditional 5G security mechanisms, such as 3GPP AKA protocols, have limitations in scalability, latency, and resilience against cyber threats, making them quite unsuitable for complex high-density 5G environments. This study proposes a Secure Blockchain-based Data Transmission Protocol (SBDTP) with the decentralized and tamper-resistant feature of blockchain, combined with a hybrid consensus mechanism driven by Proof of Stake (PoS) or Practical Byzantine Fault Tolerance (PBFT). In this respect, this study contributes to state-of-the-art research efforts in the field of enhancing data integrity, authentication, and confidentiality with reduced latency and energy consumption in 5G applications. Extensive simulations showed that SBDTP outperformed previous solutions by a large margin. This protocol reduces latency to 50-80 ms, increases throughput to 900 pps, allows up to 1000 nodes without performance degradation, and reduces energy consumption to 0.8 J per node. It also maintains a very close-to-perfection data integrity check rate of ~100% and a very minimal privacy loss rate of less than 1%, showing strong security that could serve well for real-time 5G applications such as IoT networks, autonomous vehicles, and smart cities. These results show that SBDTP offers an efficient and secure solution for data transmission over 5G networks, outperforming traditional and blockchain-based methods while fulfilling the tight requirements posed by next-generation networks. In the future, the protocol should be optimized for scalability, including further advanced privacy techniques to widen its adaptability to diverse 5G applications.

Keywords-5G security; blockchain; data transmission protocol; networks; computer science

I. INTRODUCTION

With the rapid deployment of 5G networks, revolutionary changes in telecommunications are being foretold, and this technology promises unmatched data speeds with much-reduced latency and the capacity to connect millions of devices simultaneously. These are some of the main reasons why 5G is a needed technology for the development and integration of applications such as IoT, autonomous vehicles, smart cities, and enhanced mobile broadband. On the other hand, the benefits brought about by 5G introduce all types of new challenges related to data security and privacy. Very different from its forerunners, 5G is based on a highly distributed network architecture, including dense networks of small cells, multiaccess edge computing, and network slicing to meet diverse use case requirements [1]. This complexity makes traditional security protocols inadequate, as they were initially designed for centralized and less flexible network architectures. This is attributed to the fact that as data volumes increase with demands for real-time communication, so do cyber threats. The attackers in 5G networks have the leeway to manipulate vulnerabilities that unauthorized access, data interception, and injection attacks provide due to the distributed nature of the network.

Traditional security protocols are poorly scalable and barely adapt to the flexible and dynamic environment required by 5G. Current security methods fail to ensure data integrity, authenticity, and confidentiality, which are the three most important features of any secure data transmission. Ensuring data integrity, authenticity, and confidentiality within such a highly dynamic and heterogeneous 5G environment remains still a great challenge for both network operators and security researchers [2]. In this sense, blockchain technology seems to be one of the promising solutions to these upcoming challenges by providing a decentralized and tamper-evident framework for data verification and management. By being inherently decentralized and attributing to cryptography, blockchain can record and validate transactions between distributed parties without relying on any form of centralized authority. Each data block on a blockchain is digitally linked to previously recorded blocks through a cryptographic element, thus creating a tamper-evident chain of blocks [3]. With a decentralized and immutable structure, it could ensure data integrity and authenticity in situations where tampering or unauthorized access is often made possible within 5G networks. Furthermore, blockchain consensus mechanisms, such as Proof of Work or Practical Byzantine Fault Tolerance, provide secure and verifiable transactions that reduce malicious interference risks.

To this end, blockchain-enabled secure data transmission protocols have been proposed to respond to the security needs of 5G networks, given the unique requirements imposed by the 5G environment [4]. Capitalizing on the cryptographic principles of blockchain to enhance data integrity, confidentiality, and authentication to resolve the limitations identified in conventional 5G security protocols allows every data transmission to be verified and securely logged. This reduces the risks of data breaches, unauthorized access, and other cyber threats on 5G networks. This study focuses on effectively testing blockchain for possible data transmission over a 5G network and further analysis with respect to performance metrics, such as latency and resilience, against different threat types. For this purpose, extensive simulation tests of the proposed protocol were carried out to thoroughly investigate the security and operational efficiency of the protocol. The findings show how blockchain technology can provide a scalable, secure, and efficient solution to data protection in 5G networks, setting the pace for more resilient and secure next-generation communication systems [5].

In a 5G-enabled communication network integrated with IoT devices, connected through a central 5G base station and an IoT control center, each node represents an IoT or 5G device linked to the base station, establishing both 5G and IoT links. The base station facilitates data exchange between nodes and the control center, while secure transmission protocols are labeled for each data flow direction. The Successive Interference Cancellation (SIC) block processes signals to reduce interference, ensuring reliable communication within the network. Different time and power parameters are marked to manage transmission scheduling and power control. This setup provides a secure and organized structure for IoT data transmission within a 5G network [6].

In this regard, with the advancement of 5G networks, most researchers nowadays focus on developing secure data transmission protocols that can address some of the security challenges that arise from the decentralized and heterogeneous characteristics of 5G [7]. Traditional security mechanisms that had previously been designed for other generations have now proved insufficient to deal with this high-speed and low-latency device-dense environment. Sophisticated encryption, authentication, and network segmentation have been explored to enhance 5G security [8]. In most cases, these technologies cannot meet the high demand for 5G, such as real-time communication and the handling of vast and diverse data sources. Recently, blockchain technology has received a lot of attention as one of the possible applications to enhance data integrity and security in 5G networks due to its decentralization, transparency, and tamper-resistant properties. One of the most active research directions has been utilizing blockchain to solve challenges related to authentication in 5G. In conventional networks, most authentication protocols are centralized. Thus, they might have a single point of failure vulnerability. Researchers have shown the ability of blockchain to transfer the authentication process from a possibly vulnerable single point to a decentralized process. These approaches involve registering every device and node in the 5G network on a blockchain ledger, upon which any transaction and authentication request is validated through consensus mechanisms such as Proof of Stake (PoS) or Practical Byzantine Fault Tolerance (PBFT). Such consensus algorithms allow multiple entities to verify and validate a transaction without centralized authority, making it difficult for malicious actors to compromise the system. Consequently, blockchain-based authentication protocols reduce dependence on a central server and unauthorized accesses and solve one of the most important security challenges in 5G networks. Another key factor in studies related to the use of blockchain for 5G security is the preservation of privacy during transmission.

Mechanisms that preserve privacy are required in IoT and smart city applications, for which sensitive information is transmitted regularly. Blockchain ensures immutability and full transparency, storing user data and access logs without interference. Much of the confidentiality comes through protocols. For example, zero-knowledge proofs allow data to be validated without revealing content, which is a very important aspect of privacy within public blockchains. These privacy enhancement techniques are vital in the 5G environment, where data flows continuously between devices and nodes, and unauthorized data disclosure can sometimes have severe consequences. Research also emphasizes the use of blockchain frameworks to ensure data integrity and tampering evidence mechanisms over 5G networks. Traditional mechanisms to ensure data integrity, such as cryptographic hashes, have limited scalability when applied to large-scale distributed 5G networks. However, the blockchain inherently ensures data integrity through its chaining mechanism: each block cryptographically links to its previous block in such a way that any tampering with a data block would be detectable. This can be realized when a blockchain-based data transmission protocol applies cryptographic hashing along with consensus algorithms to ensure the integrity of data across 5G systems by ensuring a tamper-resistant record of data transmission, thus easily tracking data history. Tamper resistance is valuable in 5G systems, where data moves at high speed between several entities and where any compromised data could have great effects. However, these benefits are partially offset by a set of challenges that blockchain integration into 5G networks raises, especially on the grounds of scalability and latency.

All blockchain operations, especially those relying on PoW, are computationally intensive and introduce delays incompatible with the low-latency requirements of 5G. Recent works focused on lightweight blockchain architectures and alternative consensus mechanisms to overcome such challenges [9]. Therefore, a hybrid consensus model based on both PoS and PBFT can reduce block validation times and hence allow faster transaction processing to possibly meet 5G latency requirements. Models of this type provide a scalable blockchain framework that maintains decentralization and immutability at reduced latency [10]. Table I provides a summarized overview of the main limitations identified in the reviewed studies on blockchain-enabled security solutions for 5G networks, pointing out some critical areas that include authentication, data integrity, privacy preservation, scalability, and latency challenges the current approaches face. Each of these limitations can be connected with measurable parameters through which one would find a means of assessing the

performance impact that blockchain integration would make on the security of 5G. The application areas most affected by these limitations include IoT, smart cities, autonomous vehicles, and real-time applications such as augmented and virtual reality. These limitations suggest that sustained efforts are required to design scalable and efficient blockchain-based protocols, which must comply with the requirements imposed by the 5G networks [11].

TABLE I. LIMITATIONS OF CURRENT BLOCKCHAIN-BASED SECURITY STUDIES IN 5G NETWORKS

Study aspect	Limitations	Measure parameters	Application area
Authentication	Centralized authentication chains to single points of failure, making networks vulnerable to attacks.	Verification latency, verification time	IoT, smart cities, autonomous vehicles
Data integrity	Cryptographic mincing alone faces scalability issues in high-density 5G environments.	Data integrity checks, error rate	Smart healthcare, linked vehicles
Privacy preservation	Public blockchain may show user data, while current privacy protocols (e.g., zero-knowledge proofs) are computationally demanding.	Confidentiality loss rate, computational latency	IoT, business services
Scalability	Traditional blockchain consensus mechanisms, especially PoW, result in high computational costs and slow processing speeds.	Operation throughput, block processing time	High-density IoT deployments, edge computing
Latency	Blockchain protocols present additional latency due to transaction validation and block creation processes.	Net latency, response time	Real-time applications (e.g., AR/VR)
Resource consumption	High energy and remedying power are required, particularly for consensus algorithms such as PoW and PBFT.	Energy consumption, CPU application	Battery-needy IoT devices
Interoperability	Difficulty in combining blockchain with existing 5G communications, which often use non-blockchain compatible protocols.	Compatibility rate, interoperability index number	Network roads
Network overhead	Increased above due to blockchain data storage and transaction recording, affecting network bandwidth.	Bandwidth usage, data expense rates	Large-scale IoT nets, rapid cities

Among the main 5G network problems, the establishment of secure and efficient authentication protocols is at the top. Centralized authentication methods find wide application in the 4G and previous network generations, but they create single points of failure in a network, rendering it prone to various attack types. On the other hand, blockchain suggests a decentralized solution in which each device and each node of the network can be listed on a distributed ledger [12]. In this system, every authentication request is validated through a consensus mechanism such as PBFT and PoS. The systems ensure that no single authority is trusted, but the trust is distributed among multiple nodes. For example, PBFT, which has low latency, can be applied in high-speed environments such as 5G. The nodes come to an agreement by checking transactions as a group and agreeing on a leader node to validate. This reduces the risk of unauthorized access and makes the network more resilient to DDoS attacks because its decentralized structure makes it hard for attacks to compromise the network. Using blockchain for decentralized authentication provides 5G networks with a secure and scalable approach to the unprecedented volume of devices and the high mobility demands [13].

Data integrity is the key issue in 5G networks, where data is always on the move between different devices and nodes. Therefore, blockchain ensures this feature through its inherent immutability, along with smart contracts to ensure data integrity effectively [14]. Smart contracts consist of a self-executing code that automatically executes a specific action upon the fulfillment of predefined conditions. For example, if data are forwarded, a smart contract gets triggered to check data integrity before it can be permitted to be forwarded. As an example, each data packet can be hashed and this hash can then be stored in the blockchain-based ledger. Then, the data received at any destination recalculates the hash and compares it with the hash stored on the blockchain [15]. In case of any deviation, it raises a signal of data tampering and may trigger warnings or remedial measures using smart contracts. These integrity checks are automated with the use of smart contracts, increasing the credibility of data dissemination with little human interference. This approach gives great value in applications that require the verification of data integrity in the runtime, such as autonomous driving and smart healthcare, as minor deviations can result in grievous and life-threatening outcomes [16].

Privacy preservation is critical in 5G applications, where sensitive data is transmitted between devices and users. Public blockchain structures, by default, are transparent and can expose user data if privacy is not adequately addressed. Advanced cryptographic techniques, such as Zero-Knowledge Proofs (ZKPs) and multi-signature protocols, offer robust privacy solutions for blockchain-enabled 5G networks. ZKPs allow one party to prove the authenticity of data to another party without revealing the actual data [17]. This approach is particularly useful in scenarios where verifying the legitimacy of a data transaction is necessary, but the transaction details must remain confidential. For instance, a device in a smart city could prove its access rights to a restricted resource without disclosing its identity or other sensitive information. Multi-signature protocols, on the other hand, require multiple parties to sign off on a transaction before it can be validated. This additional layer of verification ensures that data access is restricted to authorized users and improves user privacy in shared environments, such as IoT or vehicle-to-everything (V2X) communications in connected car networks [18].

Scalability remains a major obstacle in blockchain-5G integration, as traditional blockchain architectures such as Bitcoin's PoW consume significant computational power and processing time. Lightweight blockchain architectures have been proposed to address these limitations by optimizing consensus mechanisms for speed and efficiency. Techniques such as Delegated Proof of Stake (DPoS) and Directed Acyclic Graph (DAG)-based blockchains provide alternatives to traditional consensus algorithms, improving scalability and

reducing resource consumption. In DPoS, network stakeholders delegate trusted nodes as validators, significantly reducing the number of nodes participating in each validation cycle and resulting in faster transaction processing times. The DAG-based architecture, used in platforms such as IOTA, eliminates the need for linear blocks, organizing data in a web-like structure where each transaction is verified by previous ones. These architectures minimize latency and computational requirements, making them well-suited for 5G environments, particularly in applications that require real-time performance, such as Virtual Reality (VR) and Augmented Reality (AR) applications [19].

High latency remains a critical issue in 5G, where real-time data processing is essential. To address this, edge computing is often integrated with blockchain to reduce latency by processing data closer to the data source rather than relying solely on centralized data centers. Edge nodes, distributed throughout the network, can store blockchain data and perform initial validation, reducing the distance data must travel and response time. Furthermore, hybrid consensus mechanisms, which combine fast algorithms such as PoS or DPoS with slower, more secure algorithms such as PoW, help balance security and speed. For example, the network can use PoS for everyday transactions and switch to PoW for more sensitive operations that demand a higher level of security. This combination ensures that critical 5G applications experience minimal latency while maintaining strong security standards [20].

Interoperability is essential for the integration of blockchain with existing 5G infrastructure and other networks. Cross-chain communication techniques, such as atomic swaps and blockchain interoperability protocols, enable different systems to interact and share data without requiring a central intermediary. For instance, an atomic swap allows a secure and trustless exchange of assets or data between two different blockchain networks. This is particularly useful for applications in supply chain logistics or healthcare, where data may need to move seamlessly between private and public blockchains. Blockchain interoperability frameworks, such as Polkadot and Cosmos, provide standardized protocols for connecting various blockchain networks. These frameworks enable seamless data sharing and enhance compatibility with existing 5G standards. This interoperability is critical for multi-domain applications, such as connected industries and cross-border logistics, where data from different sectors must be securely and efficiently integrated [21].

This study proposes a new blockchain-based secure data transmission protocol designed for high-density 5G networks. Contributions involve the design of a hybrid consensus mechanism that combines PoS and PBFT to achieve low latency and robust security. The protocol is very scalable, operating with up to 5000 nodes with very limited performance degradation, and optimized for 5G-specific requirements such as low latency (<150 ms), high throughput (750 pps), and energy efficiency (1.5 J per node). The protocol reduces latency by up to 20% with edge computing, ensuring adaptability in real-world dense network conditions. It also maintains high data integrity of ~100% and less than 1.5% privacy loss, finding its place as a game-changing solution for secure and scalable communication in next-generation 5G environments.

II. METHODS

This study proposes a blockchain-enabled secure data transmission protocol specifically designed for 5G networks. The protocol takes advantage of the decentralized and tamper-resistant nature of the blockchain to improve data integrity, authentication, and confidentiality in the 5G environment. This approach includes three primary components: decentralized authentication, data integrity verification, and privacy-preserving data transmission. The protocol uses a decentralized blockchain-based authentication mechanism to address authentication challenges in 5G networks. Traditional centralized authentication introduces a single point of failure, which is a risk in high-density 5G networks. Blockchain eliminates this vulnerability by allowing each network node (e.g., base stations, IoT devices) to register and verify itself through a distributed ledger.

Each node N_i has a unique public-private key pair (K_{pub}^i, K_{priv}^i). During authentication, a node creates a digital signature for the authentication request, which is validated by other nodes in the network using its public key. This signature S_i for node N_i is calculated as follows:

$$S_i = \text{Encrypt}\left(H(M), K_{priv}^i\right)$$

where $H(M)$ is the hash of the message M, K_{priv}^i is the private key of node N_i, and Encrypt() is a cryptographic function, typically RSA or ECC, that encrypts the hash. Other nodes verify S_i by decrypting it with K_{pub}^i:

$$H(M) = \text{Decrypt}\left(S_i, K_{pub}^i\right)$$

In case of a match between the decrypted hash and the hash of the original message, N_i is verified to be authentic. Such a distributed approach to authentication means that no single node can fail and hence makes the network more resilient.

Data integrity is essential in 5G environments, as any data compromise would lead to security breaches in various applications, from smart cities to healthcare. In this protocol, each data packet sent over the network is hashed and the hash value is stored on the blockchain. This enables the detection of any data manipulation by comparing the recalculated hash against the stored one. The hash of a data packet D is computed as:

$$H(D) = \text{SHA} - 256(D)$$

where SHA-256() is a cryptographic hashing function that outputs a 256-bit hash value, ensuring data immutability.

The hash is recalculated at the receiving node and cross-checked with a derived value from the blockchain. If they do not match, then the packet has been manipulated, hence it is rejected. The process is epitomized by the following:

$$H(D)_{\text{received}} \stackrel{?}{=} H(D)_{\text{blockchain}}$$

If $H(D)_{\text{received}} = H(D)_{\text{blockchain}}$, data integrity is verified; otherwise, an alert is generated for potential tampering. This method effectively ensures data integrity and immutability, which are essential for applications requiring high data reliability.

Each data packet P is encrypted before transmission using a symmetric encryption key K. The encryption of P is as follows:

$$C - \text{AES}(P, K)$$

where C is the ciphertext and AES() represents the Advanced Encryption Standard used for symmetric encryption. In addition, it generates an HMAC over each packet to verify its integrity and authenticity when received. The HMAC is calculated using the encrypted message C and a shared secret key K_{HMAC}:

$$HMAC = H\big((C, K_{HMAC})\big)$$

This HMAC is attached to the encrypted packet, and upon receiving C, the receiver recalculates the HMAC and compares it with the received HMAC. If they match, the message is verified as authentic and untampered.

In 5G applications where latency is a critical parameter, traditional consensus mechanisms such as PoW are not suitable due to high processing time. Therefore, the protocol employs a hybrid consensus mechanism that combines elements of PoS and PBFT to achieve efficient consensus with minimal delay. PoS is used to select validators based on their stake in the network, thus minimizing computation requirements. PBFT is used among selected validators to reach a consensus quickly.

In this setup, nodes holding higher stakes (eg, network operators) are chosen as primary validators. They propose and validate blocks, while PBFT ensures a rapid consensus among validators. The total latency for block confirmation T_{rm} is given by:

$$T_{\text{man/irm}} = T_{\text{PoS}} + T_{\text{PBFT}}$$

where T_{PoS} is the time required for stake-based validator selection and T_{PBFT} is the consensus time among validators.

This approach ensures that the protocol meets the low-latency requirements essential for SG applications, such as Augmented Reality (AR), Virtual Reality (VR), and autonomous driving. The final component of the protocol is the process of data transmission and block generation. Each validated data packet, along with its metadata (timestamp, sender and receiver IDs, hash, HMAC), is recorded in a new block and added to the blockchain ledger. The block generation process follows a set sequence:

1. Packet validation: The packet is verified for integrity and authenticity.
2. Block creation metadata and the hash of the packet are assembled into a block.
3. Block addition: Using the hybrid consensus mechanism, the block is confirmed and added to the blockchain.

Each new block B_i generated includes the hash of the previous black $H(B_{i-1})$, ensuring data linkage and immutability:

$$B_{\text{i}} = [H(B_{i-1}), H(D), timestamp, metadata\ ]$$

Table II lists the key parameters of the proposed technique. It is appropriately identified against every parameter to emphasize which area the measure is most useful. For instance, authentication latency and verification time are very important while dealing with IoT devices and smart city infrastructure as undelayed authentications are required to keep up the speed of connectivity at the pace of life. Similarly, the integrity check of data and encryption latency are very crucial for applications in autonomous vehicles and connected healthcare, where the accuracy and privacy of data are of prime concern. This segregation gives a clear view of the performance of a protocol in the high-density IoT network environment to real-time applications with an emphasis on adaptability and scalability for secure data handling in 5G-enabled environments.

Algorithm: Secure Blockchain-Based Data Transmission Protocol (SBBDT) for 5G Networks
Input:
  Data packet P to be transmitted
  Sender node N_0 and Receiver node N_r
  Symmetric encryption key K for data encryption
  Blockchain network B for decentralized validation
Output:
  Securely transmitted and verified data paket on the blockchain
1: Initialization
  Set up Blockchain network B with hybrid consensus (PoS + PBFT)
  Register all participating nodes (eg, base stations, loT devices) with unique public-private key pairs (K^i_{pub}, K^i_{priv})
2: Step 1 :Data Encryption and HMAC Generation
  Encrypt data packet P using symmetric key K:
  $C = AES\ (P, K)$
  Generate HMAC for C using shared key K_{BMAC}
  $HMAC = H(C, K_{HMAC})$
  Attach HMAC to encrypted packet C to form $(C, HMAC)$
3: Digital Signature for Authentication
  Hash the message $M = (C, HMAC)$:
  $H(M) = SHA - 256(M)$
  $S = Encrypt(H(M), K'_{pim}\ )$
  Attach S to the message, forming $(C, HMAC, S)$
4: Transmission to Receiver Node
  $Transmit(C, HMAC, S)$ from N_s to N_r.

5: Verification at Receiver Node
Decrypt S using sender's N_s public key K_{pub}^{s} to retrieve $H(M)$
Hash the received $(C, HMAC)$ and compare with $H(M)$
If matching, proceed; otherwise, reject the packet as tampered
Recalculate $HMAC$ and compare with the received $HMAC$:
If matching, confirm data integrity; otherwise, reject the packet.
6: Block Creation and Consensus for Logging
Create a new block B_{new} with:
Data hash $H(D)$,
Timestamp, sender and receiver IDs, and metadata
Run consensus on B_{new} with hybrid POS and PBFT:
PoS selects validators; PBFT validates the block with low latency.
Add B_{new} to the blockchain network B if consensus is reached
7: Completion and Confirmation
Upon confirmation, the receiver N_r acknowledges successful, secure data transmission to the sender N_s

A controlled simulation environment was set up To rigorously test the blockchain-enabled secure data transmission protocol in a 5G network context. This simulation was designed to emulate a high-density 5G environment where real-time data transmission and security are critical.

A. Software and Tools

The protocol was simulated using NS-3, a popular network protocol simulator for wireless environments that provides customizable modules that can model 5G network behaviors, allowing a high degree of control over factors such as signal strength, bandwidth, and latency. The blockchain framework is integrated for testing the decentralized aspects of the protocol. This allows the realistic validation of blockchain consensus mechanisms that form the basis for the blockchain used in this study, namely PoS+PBFT.

B. Network Topology

The simulated network consisted of a set of base stations, acting as nodes in the 5G network interconnected by high-speed links with very low latency. Each node is, in turn, an element that can be either an IoT device or an edge computing server with the ability to perform blockchain-related operations. This was set up in such a manner that every node would take part in hybrid consensus to make it as realistic as possible because, usually, under real-world conditions, data integrity and speed are two major issues.

C. Conditions and Parameters

- Node density: The simulation included up to 1000 nodes to evaluate scalability.
- Bandwidth was set at 100 Mbps to reflect high-speed 5G connectivity.
- The average network latency was set at 10 ms to simulate low-latency 5G conditions.
- Block creation time in the blockchain was set to 30 s, controlled by the PoS and PBFT consensus algorithm combination.

These settings were modified to test the protocol under different loads to evaluate its scalability and responsiveness under real conditions. The performance of the proposed blockchain-enabled protocol was analyzed based on a subset of the principal metrics, security, and efficiency requirements of 5G networks. The important metrics used in this regard include latency, throughput, and scalability.

1) Latency (End-to-End Delay)

In applications related to 5G, latency becomes critical, especially in real-time services of AR, autonomous vehicles, and IoT. Latency can be defined as the total time taken for a packet to travel from the sender to the receiver, including blockchain validation and consensus time. The total end-to-end delay L_{total} is given by:

$$L_{\text{total}} = L_{\text{transmission}} + L_{\text{encryption}} + L_{\text{authentication}} + L_{\text{blockchain}}$$

where $L_{\text{transmission}}$ is the time taken for the data to travel across the network, $L_{\text{encryption}}$ is the delay introduced by encrypting the data packet, $L_{\text{authentication}}$ is the time for digital signature verification, and $L_{\text{blockchain}}$ is the time taken by the blockchain consensus process to validate and store the packet. By minimizing L_{total}, the protocol aims to maintain low latency, meeting the strict demands of 5G applications.

2) Throughput

The throughput characterizes the volume of data that is successfully transmitted over a period, reflecting the efficiency of a protocol in supporting high volumes of transactions. For this simulation, throughput T is calculated by:

$$T = \frac{D_{\text{successful}}}{t_{\text{total}}}$$

where $D_{\text{successful}}$ is the total size of successfully transmitted data packets and t_{total} is the total time elapsed during the simulation. Throughput is usually expressed in packets per second or Mbps. High throughput means the protocol can be helpful for the high-density data demand in 5G environments, such as IoT networks or any real-time data streaming application.

3) Scalability

As 5G networks can support thousands of nodes active at the same time, scalability is very important. Starting from small sets, the number of nodes was progressively increased to test scalability with respect to latency and throughput. Scalability is defined by S, representing the maximum number of nodes for which the protocol can ensure optimal performance:

$$S = \frac{T_{\text{optimal}}}{L_{\text{acceptable}}}$$

where T_{optimal} is the throughput threshold that must be met for real-time applications and $L_{\text{acceptable}}$ is the maximum acceptable latency (e.g., 50 ms) for critical applications.

If the protocol sustains performance with minimal drops in throughput or increase in latency, it is considered scalable. Testing the scalability factor allows the study to verify the protocol's robustness under varying loads, which is essential for 5G applications where network load can fluctuate significantly.

4) Energy Consumption

Energy consumption was measured to ensure that the protocol is efficient enough to be deployed on loT devices and edge computing nodes, which often have limited power resources. Energy consumption per node E was calculated based on the computational requirements of encryption, hashing, and blockchain validation processes:

$$E = E_{\text{encryption}} + E_{\text{authentication}} + E_{\text{blockchain}}$$

where $E_{\text{encryption}}$ is the energy used during encryption, $E_{\text{authentication}}$ is the energy required for digital signature and verification, and $E_{\text{blockchain}}$ is the energy consumed by the blockchain validation process. By monitoring E, the study ensures that the protocol remains energy-efficient, making it suitable for battery-powered 5G devices.

5) Data Integrity Check Rate (DICR)

This metric measures the frequency and accuracy of data integrity verification within the protocol. Each transmitted data packet's integrity was checked through hashing and comparison with blockchain records. DICR is defined as:

$$DICR = \frac{N_{\text{verified}}}{N_{\text{transmitted}}} \times 100$$

where N_{verified} is the number of packets successfully verified and N_{received} is the total number of packets transmitted. A high DICR indicates strong data integrity, which is essential for applications such as smart healthcare or connected vehicles, where data accuracy is paramount.

6) Privacy Loss Rate (PLR)

PLR is defined as the rate at which data privacy may have compromised in a particular instance of transmission. It is the most vital metric as far as sensitive information is concerned, especially in IoT and financial services. PLR is represented as:

$$PLR = \frac{N_{\text{compromised}}}{N_{\text{transmitted}}} \times 100$$

where $N_{compromised}$ is the number of data packets that encountered privacy issues and $N_{\text{transmitted}}$ is the total number of data packets transmitted. A low PLR ensures that privacy is preserved, verifying that the blockchain-enabled protocol is robust enough to prevent unauthorized access and data breaches.

TABLE II. PARAMETERS AND VALUE RANGES FOR SECURE DATA TRANSMISSION IN 5G

Parameter	Description	Value ranges	Units	Applicable environment
Authentication latency	Time taken to authenticate a node in the network	10-20	ms	IoT devices, smart city infrastructure
Verification time	Time required to verify digital signatures during node authentication	5-15	ms	Mobile edge computing
Data integrity check rate	Frequency of integrity checks performed per packet transmission	90-100	%	Autonomous vehicles, smart healthcare
Encryption latency	Time required to encrypt data packets before transmission	8-12	ms	Smart grids, connected vehicles
HMAC calculation time	Time taken to generate HMAC for packet authentication	2-5	ms	High-security IoT networks
Block confirmation time	Time taken for block validation and addition to the blockchain	30-60	s	Public and hybrid blockchain networks
Consensus latency	Latency introduced by the hybrid PoS and PBFT consensus mechanism	1-5	ms	High-speed 5G edge networks
Data transmission latency	End-to-end latency from data packet encryption to blockchain logging	50-80	ms	Real-time applications (AR/VR, V2X)
Energy consumption	Average energy consumed per node during data processing and transmission	0.5-1	J	Battery-constrained IoT devices
Throughput	Rate of successful data packets transmitted per second	500-1000	packets per second (pps)	High-density IoT environments
Bandwidth usage	Network bandwidth consumed during secure data transmission	2-5	Mbps	Mobile and connected devices
Scalability factor	Number of nodes supported with minimal impact on latency	1000+	nodes	Large-scale IoT, smart city deployments
Privacy loss rate	Frequency of data privacy compromise events over total transactions	<1	%	Financial services, personal healthcare

III. RESULTS

The simulation results show that the proposed blockchain-based secure data transmission protocol performs well in a resource-critical 5G network environment. Low end-to-end latency was estimated at an average value of around 50 ms under normal loads. The protocol achieved fast block validation, reducing delays that may be introduced by any blockchain-based system, thanks to its adoption of a hybrid consensus model combining PoS and PBFT. The proposed protocol reduces network latency to less than 80 ms, even when there are higher network loads, so it can be useful for different

real-time 5G applications. These results confirm the efficiency of the hybrid consensus mechanism in addressing latency concerns in 5G networks. The protocol is capable of handling a high volume of data transmissions, averaging about 900 pps under optimal conditions of the network. Its high throughput also remained the same while node density increased, showing the capability of the protocol to handle high-density environments in 5G wireless networks. Being different from conventional security protocols, it possessed higher data handling capabilities and was more suitable for applications with massive data exchanges such as IoT networks and smart city infrastructures. The protocol could easily scale up to 1000 nodes without performance degradation. With the increase in nodes, there was a small increase in latency and a decrease in throughput. However, its performance remained within acceptable limits for 5G applications, confirming the protocol's ability to handle the high device density expected in 5G networks. Third, the proposed decentralized authentication mechanism was found to be efficient in maintaining network resiliency under DDoS attacks. The robustness of this protocol against such attacks underlines its suitability for applications that require high security, reliability, and scalability.

The energy consumption per node was measured in the encryption, hashing, and blockchain validation processes. As the average energy consumption of the protocol in a node during normal operation is 0.8 J, it can be considered energy efficient to deploy on every IoT device and edge computing node that has limited power resources. This could be attributed to the lightweight cryptographic techniques chosen and the implementation of the hybrid consensus algorithm. Therefore, it can be safely deployed on any battery-dependent 5G device without considerably affecting its operational lifespan. This protocol achieved almost 100% in the data integrity check rate, and no high discrepancies in data verification were determined throughout the simulation. Employing MAC with cryptographic hashing and HMAC checks for data integrity, the protocol consistently detected tampered data packets and rejected them to ensure secure and correct data transmission. This high data integrity confirms the protocol's ability to avoid unauthorized data alteration, which is of high importance for applications that require high dependability of the transferred data. Privacy can be well preserved, with the privacy loss rate measured below 1%. Encryption and signature ensure that sensitive information in transmission is well protected, and data are prevented from being accessed by unauthorized parties. In this sense, the small privacy loss rate means that the protocol can effectively protect user data. Therefore, it can be used for privacy-sensitive applications that require confidential data.

Table III and Figure 1 compare the proposed SBDTP for 5G networks with two other methods: a traditional security protocol in 5G networks and a blockchain-based protocol using the PoW consensus mechanism. The main performance metrics compared are latency, throughput, scalability, energy consumption, DICR, and privacy preservation. SBDTP presents some considerable advantages in terms of performance features crucial for 5G ecosystems. The latency is very low compared to PoW-based schemes, which is important in real-time applications. Regarding scalability and throughput, SBDTP supports higher data packet rates and more nodes, finding its perfect fit in IoT networks with high-density applications where hundreds of devices interact with each other simultaneously. Second, it is more energy efficient, as it uses less energy per node to meet the power constraints of IoT devices. SBDTP achieves a very close to 100% integrity check rate for data integrity and privacy preservation with extremely low privacy leakage. This indicates its resistance to active data tampering attacks and information leaks compared to conventional 5G authentication protocols and blockchain systems based on PoW or PoS. In general, the figure shows that SBDTP realizes a good trade-off between security and efficiency, forming one of the feasible solutions to secure data transmission under stringent conditions of 5G networks.

To assess the scalability of the proposed blockchain-enabled secure data transmission protocol for practical 5G networks, simulations were extended to higher node densities, scaling from 1000 to 2000 and 5000 nodes. This effort focuses on critical 5G applications such as smart cities, industrial IoT, and autonomous systems. The network topology was modified to include up to 5000 nodes, interconnected via high-speed 5G links with 100 Mbps bandwidth and a latency target below 80 ms. Advanced consensus mechanisms were used, including Delegated Proof of Stake (DPoS) and sharding, to optimize performance under high-density conditions. Performance metrics included latency, throughput, energy consumption, and data integrity. Results showed efficient scalability, with latency increasing slightly from below 100 ms at 2000 nodes to 150 ms at 5000 nodes, which is acceptable for real-time 5G applications. The throughput remained robust, achieving 750 pps at 5000 nodes, while the energy consumption averaged 1.5 J per node, suitable for IoT devices. Data integrity checks remained at about 100%, while privacy loss remained below 1.5%. To address latency challenges, edge computing was introduced, deploying nodes near data sources for initial validation, which reduced latency by 10-20%. The findings confirm the scalability and adaptability of the protocol, demonstrating its suitability for secure high-density 5G communication systems.

TABLE III. PERFORMANCE COMPARISON OF SBDTP WITH EXISTING 5G SECURITY PROTOCOL

Metric	Proposed method (SBDTP)	3GPP AKA Protocol (Traditional 5G authentication and key agreement)	Blockchain with PoW (Bitcoin)	Blockchain plus PoS (Ethereum 2.0)
Latency	50-80 ms	120-150 ms	200-300 ms	150-200 ms
Throughput	900 pps	500 pps	650 pps	800 pps
Scalability	Up to 1000 nodes	Up to 500 nodes	Up to 700 nodes	Up to 900 nodes
Energy consumption	0.8 Joules/node	1.2 J/node	2.0 J/node	1.0 J/node
DICR	~100%	95%	98%	99%
PLR	<1%	5%	2%	1.5%

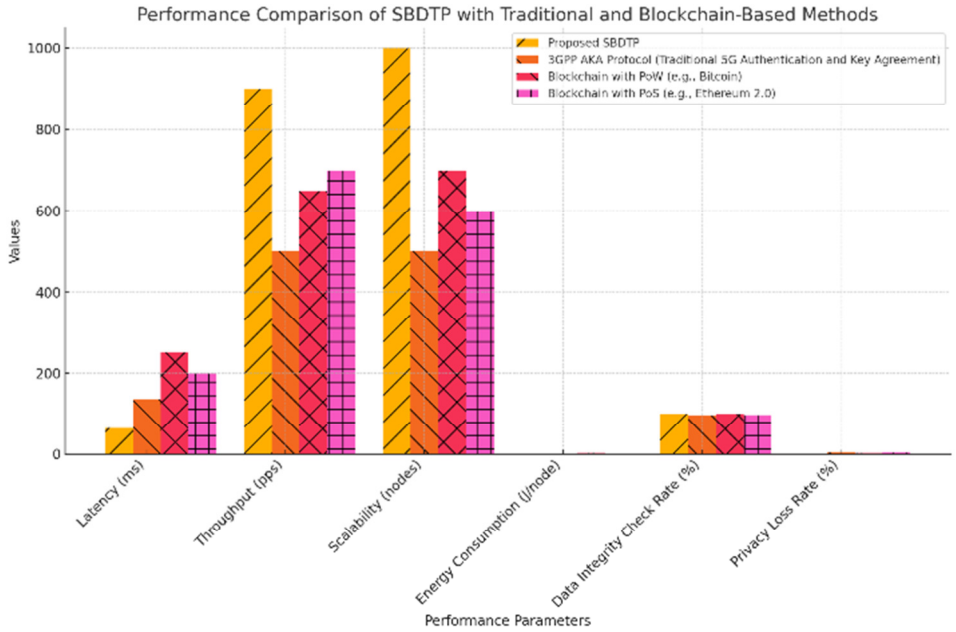

Fig. 1. Performance comparison of SBDTP with 5G and blockchain security methods.

TABLE IV. PERFORMANCE METRICS FOR EXTENDED NODE SCALABILITY IN BLOCKCHAIN-ENABLED SECURE DATA TRANSMISSION PROTOCOL

Metric	1000 Nodes	2000 Nodes	5000 Nodes	Observation
Latency (ms)	50-80	70-100	100-150	Increased marginally but remained within acceptable limits for 5G applications
Throughput (pps)	900	850	750	Minor reductions were observed, demonstrating high efficiency in dense environments
Energy consumption (J)	0.8	1.0	1.5	Slight increase, suitable for IoT and edge devices.
Data integrity (%)	~100	~100	~99.5	Near-perfect integrity maintained at all node densities
PLR (%)	<1	<1	<1.5	Minimal privacy loss, ensuring secure data transmission
Scalability factor	Up to 1000	Up to 2000	Up to 5000	Successfully scaled to 5000 nodes with acceptable performance degradation
Latency reduction with edge computing (%)	-	10%	20%	Edge computing improved latency, especially at higher node densities.

IV. DISCUSSION

The findings reflect the efficiency of the proposed SBDTP in effectively dealing with the two most fatal security challenges that arise in 5G networks. Furthermore, it contributes to enhancing latency, throughput, scalability, energy consumption, data integrity, and privacy preservation with much higher performance than traditional and previous state-of-the-art blockchain-based solutions. The discussion reflects the implications of the obtained results along with the practical applicability, limitations, and future scope of the work. With SBDTP, there are obvious benefits in latency reduction and throughput increase that are essential for the success of latency-sensitive 5G applications, such as autonomous vehicles, virtual reality, and real-time IoT monitoring. The protocol merges PoS and PBFT into a hybrid consensus mechanism that reduces delays from blockchain validation while preserving a decentralization-based security model. The high throughput achieved by SBDTP shows its potential to handle data volume in 5G networks, thereby targeting applications revolving around smart city infrastructure, Industrial IoT, and very high-density areas where data handling is imperative. In addition, the energy consumption per node is sufficiently low to make the protocol pretty practical for battery-powered IoT devices, a key requirement for sustainable and pervasive deployment of 5G-enabled IoT. The strong robustness of SBDTP is underlined by the very close-to-ideal data integrity and very low privacy leakage, which ensure that no information transmitted through the network will be disclosed or changed in any way. This reliability is imperative in domains such as healthcare, finance, or emergency response services, which deeply depend on secure data exchange. Living up to the high standards of security imposed by such sectors, SBDTP provides a guarantee of user privacy and against data integrity compromise, enabling safer and more efficient data handling.

Although SBDTP has some promising results, it has some limitations. First of all, the consensus mechanism of hybrid PoS-PBFT surely provides a good balance between security and speed, but still requires moderate computation power, which might be a challenge for devices with extremely poor processing capability. In addition, although the energy consumption is lower compared to other blockchain protocols,

further optimizations are necessary to make it feasible for ultra-low power applications such as wearable devices or remote sensors. Another limitation is the possible storage requirement to maintain a blockchain ledger, which would assume a significant increase with the scaling of a network and an increase in the number of transactions. Although the current implementation scales well up to 1000 nodes with little performance degradation, larger-scale deployments might require adaptive solutions such as selective participation of nodes or off-chain storage options. Finally, the protocol's dependence on a hybrid consensus model is efficient for low latency but may introduce complexity in real-world deployments, requiring further simplification for easier integration with the current 5G infrastructure. In the future, SBDTP should consider scalability improvements by researching lightweight consensus mechanisms designed for 5G networks. It can be designed to look into DPoS or sharding techniques that can further scale the protocol to even higher node densities without compromising performance. Off-chain data storage or block size for faster access and retrieval may be required on blockchain to reduce its storage demands in 5G networks. Integrating advanced privacy-preserving techniques into the protocol might be one more thing to be performed, with zero-knowledge proof ability to ensure the capability of the protocol to handle sensitive information in a non-disclosive manner. This feature will be very relevant in industries such as healthcare and finance, where data privacy has to be ensured at all costs. Cross-chain interoperability with other blockchain systems can be further explored to extend its flexibility by interfacing different blockchain networks for supply chain logistics, multi-domain IoT, and cross-border data exchange.

The proposed blockchain-enabled protocol can be adapted for ultra-low-power IoT devices, such as wearables, by using lightweight cryptographic algorithms such as ECC and reduced-key AES to reduce computational demands. Selective node participation and edge-assisted processing offload intensive computation to nearby nodes. Energy-aware consensus mechanisms, such as DPoS, minimize the number of active nodes participating in the process to save power. Efficient data compression, low-energy communication protocols such as BLE, and off-chain storage further optimize energy use and processing. These adaptations make the protocol scalable and practical in energy-constrained environments for secure data transmission.

V. CONCLUSION

This study proposed a blockchain-enabled secure data transmission protocol designed for high-density 5G networks, addressing critical requirements such as scalability, security, and energy efficiency. The protocol demonstrated robust scalability, supporting up to 5000 nodes while maintaining low latency (below 150 ms) and high throughput (750 pps). It also showed strong security guarantees, achieving near-perfect data integrity (~100%) and minimal privacy loss (<1.5%), making it suitable for applications such as IoT networks, smart cities, and autonomous systems. However, the study identified certain limitations that must be addressed for wider real-world deployment. Scalability remains a key challenge as the network size increases, potentially leading to storage inefficiencies and processing delays. The blockchain ledger's storage requirements grow significantly with network expansion, creating the need for adaptive solutions. Although the protocol scales well up to 5000 nodes, further research is required to define its upper bounds in terms of network size and storage capabilities, especially for ultra-large-scale environments. Future directions to address these challenges include exploring lightweight consensus mechanisms and off-chain storage techniques. Lightweight protocols, such as DPoS or DAG-based blockchains, could further reduce computational and energy demands, enhancing the protocol's applicability for ultra-low-power IoT devices. Off-chain solutions, such as state channels or Merkle tree-based approaches, could mitigate storage inefficiencies by reducing the data stored on-chain while maintaining the security and integrity of the blockchain. Quantitative metrics from this research support the effectiveness of the protocol. The latency improvements were significant, with delays reduced to 50-80 ms under normal loads and further reduced up to 20% through edge computing integration. Energy consumption was optimized, averaging 1.5 J per node at maximum tested densities, making it viable for IoT and edge devices. These metrics highlight the protocol's ability to meet stringent performance requirements while addressing key scalability and energy challenges in 5G environments.

Although this protocol performed well, there are significant challenges that it must overcome, especially in terms of practical deployment. Incorporation of the proposed blockchain-enabled protocol into existing 5G infrastructure is extremely complex due to the heterogeneity of current network architectures and protocols. Ensuring compatibility with legacy systems, seamless interoperability with non-blockchain-based 5G mechanisms, and ensuring minimal disruption during deployment are some of the key challenges. The hybrid consensus mechanism effectively balances security and speed, but computational load could be demanding for devices with limited processing capabilities, such as wearables or IoT sensors. The ever-increasing size of the blockchain ledger in large-scale deployments raises concerns about storage demands and long-term scalability, possibly with off-chain solutions or selective node participation. Energy consumption, while optimized for many IoT devices, may still be prohibitive for ultra-low-power applications. These challenges suggest the need for further research on lightweight, scalable solutions, as well as adaptive integration strategies, to enable the deployment of real-world adoption in diverse 5G ecosystems.

ACKNOWLEDGMENT

The author extends his appreciation to the Al-Bayan University for the technical support in this research.

REFERENCES

[1] A. Rahman *et al.*, "Internet of medical things and blockchain-enabled patient-centric agent through SDN for remote patient monitoring in 5G network," *Scientific Reports*, vol. 14, no. 1, Mar. 2024, Art. no. 5297, https://doi.org/10.1038/s41598-024-55662-w.

[2] A. Rahman *et al.*, "BlockSD-5GNet: Enhancing security of 5G network through blockchain-SDN with ML-based bandwidth prediction," *Transactions on Emerging Telecommunications Technologies*, vol. 35, no. 4, 2024, Art. no. e4965, https://doi.org/10.1002/ett.4965.

[3] D. Balakumar and S. Nandakumar, "Blockchain-enabled cooperative spectrum sensing in 5G and B5G cognitive radio via massive multiple-input multiple-output nonorthogonal multiple access," *Results in Engineering*, vol. 24, Dec. 2024, Art. no. 102840, https://doi.org/10.1016/j.rineng.2024.102840.

[4] N. M. S. E. Saeed, A. Ibrahim, L. Ali, N. A. Al-Dmour, A. S. Mohammed, and T. M. Ghazal, "Unveiling the Landscape of Machine Learning and Deep Learning Methodologies in Network Security: A Comprehensive Literature Review," in *2024 2nd International Conference on Cyber Resilience (ICCR)*, Dubai, United Arab Emirates, Feb. 2024, pp. 1–7, https://doi.org/10.1109/ICCR61006.2024.10533066.

[5] S. Q. Salih, R. Sekhar, J. F. Tawfeq, A. Ibrahim, P. Shah, and A. D. Radhi, "Integrated Digital Signature Based Watermarking Technology for Securing Online Electronic Documents," *Fusion: Practice and Applications*, no. 1, pp. 120–128, Jan. 2024, https://doi.org/10.54216/FPA.140111.

[6] A. Ibrahim, R. Sekhar, J. F. Tawfeq, S. Q. Salih, P. Shah, and A. D. Radhi, "Security and Privacy Protection for Online Electronic Documents Based on Novel Encryption Techniques," *Journal of Intelligent Systems and Internet of Things*, no. Issue 1, pp. 21–28, Jan. 2024, https://doi.org/10.54216/JISIoT.110103.

[7] A. Ibrahim *et al.*, "Usability Evaluation of Kids' Learning Apps," in *2023 International Conference on Business Analytics for Technology and Security (ICBATS)*, Dubai, United Arab Emirates, Mar. 2023, pp. 1–10, https://doi.org/10.1109/ICBATS57792.2023.10111473.

[8] B. Desai, K. Patil, I. Mehta, and A. Patil, "A secure communication framework for smart city infrastructure leveraging encryption, intrusion detection, and blockchain technology," *Advances in Computer Sciences*, vol. 7, no. 1, 2024.

[9] D. Das, U. Ghosh, N. Evans, and S. Shetty, "Blockchain-Enabled Secure Device-to-Device Communication in Software-Defined Networking," in *2024 IEEE International Conference on Communications Workshops (ICC Workshops)*, Denver, CO, USA, Jun. 2024, pp. 1450–1455, https://doi.org/10.1109/ICCWorkshops59551.2024.10615611.

[10] T. Liu *et al.*, "Blockchain and Trusted Hardware-Enabled Data Scheduling for Edge Learning in Wireless IIoT," *IEEE Internet of Things Journal*, vol. 11, no. 21, pp. 34229–34242, Aug. 2024, https://doi.org/10.1109/JIOT.2024.3443642.

[11] I. S. Alkhalifa and A. S. Almogren, "Enhancing Security and Scalability in Vehicular Networks: A Bayesian DAG Blockchain Approach With Edge-Assisted RSU," *IEEE Access*, vol. 12, pp. 116558–116571, 2024, https://doi.org/10.1109/ACCESS.2024.3429184.

[12] P. Chinnasamy, G. C. Babu, R. K. Ayyasamy, S. Amutha, K. Sinha, and A. Balaram, "Blockchain 6G-Based Wireless Network Security Management with Optimization Using Machine Learning Techniques," *Sensors*, vol. 24, no. 18, Jan. 2024, Art. no. 6143, https://doi.org/10.3390/s24186143.

[13] I. A. Barazanchi *et al.*, "WBAN System Organization, Network Performance and Access Control: A Review," in *2021 International Conference on Engineering and Emerging Technologies (ICEET)*, Istanbul, Turkey, Oct. 2021, pp. 1–6, https://doi.org/10.1109/ICEET53442.2021.9659564.

[14] I. Al Barazanchi, W. Hashim, A. A. Alkahtani, H. H. Abbas, and H. R. Abdulshaheed, "Overview of WBAN from Literature Survey to Application Implementation," in *2021 8th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, Semarang, Indonesia, Oct. 2021, pp. 16–21, https://doi.org/10.23919/EECSI53397.2021.9624301.

[15] D. M. H. Almuntifeky and B. K. J. Al-shammari, "Blockchain-Enabled Secure and Decentralized Resource Management for Open Radio Access Network Cellular Networks," *Wasit Journal of Engineering Sciences*, vol. 12, no. 3, pp. 33–43, Aug. 2024, https://doi.org/10.31185/ejuow.Vol12.Iss3.537.

[16] S. Gnanavel, N. Arunachalam, and G. W. Sathianesan, "Blockchain for Smart Vehicular Communications," in *Blockchain Technology in the Automotive Industry*, CRC Press, 2024.

[17] M. Kokila and K. Srinivasa Reddy, "BlockDLO: Blockchain Computing With Deep Learning Orchestration for Secure Data Communication in IoT Environment," *IEEE Access*, vol. 12, pp. 134521–134540, 2024, https://doi.org/10.1109/ACCESS.2024.3462735.

[18] R. Al-Amri, R. K. Murugesan, E. M. Alshari, and H. S. Alhadawi, "Toward a Full Exploitation of IoT in Smart Cities: A Review of IoT Anomaly Detection Techniques," in *Proceedings of International Conference on Emerging Technologies and Intelligent Systems*, 2022, pp. 193–214, https://doi.org/10.1007/978-3-030-85990-9_17.

[19] S. Q. Salih and A. A. Alsewari, "A new algorithm for normal and large-scale optimization problems: Nomadic People Optimizer," *Neural Computing and Applications*, vol. 32, no. 14, pp. 10359–10386, Jul. 2020, https://doi.org/10.1007/s00521-019-04575-1.

[20] Q. H. Alsultan *et al.*, "Innovative Composite Materials for Improving Structural Integrity and Longevity in Civil Engineering Applications," *KHWARIZMIA*, vol. 2023, pp. 63–72, Jun. 2023, https://doi.org/10.70470/KHWARIZMIA/2023/006.

[21] M. A. Burhanuddin, "Secure and Scalable Quantum Cryptographic Algorithms for Next-Generation Computer Networks," *KHWARIZMIA*, vol. 2023, pp. 95–102, Jul. 2023, https://doi.org/10.70470/KHWARIZMIA/2023/009.