IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 27 December 2024, accepted 15 March 2025, date of publication 25 March 2025, date of current version 8 April 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3554643

RESEARCH ARTICLE

Blockchain-Enhanced Attribute-Based Encryption Architecture With Feasibility Analysis

AGUSTIN FERRER-ROJAS, BODHASWAR T. MAHARAJ, (Senior Member, IEEE), AND MDUDUZI C. HLOPHE

Department of Electronic, Electrical, and Computer Engineering, University of Pretoria, Pretoria 0002, South Africa

Corresponding author: Agustin Ferrer-Rojas (agufero@gmail.com)

ABSTRACT In today's digital landscape, data security is critical, particularly in the Internet of Things (IoT), where large volumes of sensitive data are exchanged. Traditional encryption methods like RSA and AES face challenges in balancing security and performance, exposing systems to advanced cyber threats. To address these issues, blockchain technology offers decentralized, tamper-resistant data protection that enhances trust and transparency. Attribute-Based Encryption (ABE) schemes have been developed, often combining asymmetric and symmetric encryption for efficiency and security. However, gaps remain in practical deployment due to underexplored network architectures and limited feasibility simulations. This study proposes an end-to-end security architecture integrating ABE with Linear Secret Sharing Scheme (LSSS) access policies and blockchain-based distributed key management. The system's feasibility was evaluated using Network Simulator 3 (NS3) within a simulated IoT network. Results demonstrate a lightweight and scalable solution suitable for constrained environments. Numerical simulations showed consensus times as low as 0.25 seconds for key agreement and 0.7 seconds for message consensus, even in resource-constrained settings. For large networks, consensus times reached as low as 0.75 seconds. The system also achieved an average throughput of 0.3 transactions per second in low-resource environments. These outcomes highlight the system's potential for secure, efficient data transmission in IoT and other distributed systems.

INDEX TERMS Access control, consensus algorithms, Internet of Things, NS3, Paxos, PBFT, Raft.

I. INTRODUCTION

The rapid expansion of Internet of Things (IoT) environments across sectors such as healthcare, agriculture, and power generation has brought significant improvements in automation and operational efficiency. However, as the number of IoT devices increases, so too does the volume of sensitive data they generate and transmit across networks. Ensuring the security of this data has become a critical challenge, especially as traditional data security methods struggle to scale effectively in larger, more complex networks [1], [2]. As IoT networks expand, there is a growing need for encryption solutions that are lightweight, secure, and scalable, capable of protecting sensitive information without imposing excessive computational overhead [3], [4].

Traditional encryption methods, such as the Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) algorithms, have long been foundational to data security. Yet, in IoT environments, these methods encounter significant limitations. A core challenge is scalability: RSA, an asymmetric algorithm known for secure key exchanges, requires large key sizes to ensure robust security, leading to high computational demands that IoT devices—often resource-constrained—struggle to support [4], [5]. While AES, a symmetric encryption method, is computationally efficient and performs well in general applications, it lacks built-in support for dynamic access control, which is critical in large-scale and diverse IoT networks [3]. Moreover, both AES and RSA generate considerable computational overhead, affecting performance in constrained network environments. Consequently, these traditional methods are increasingly seen as inadequate for the scalability, adaptability, and performance demands of IoT security frameworks, underscoring the need for more advanced encryption solutions [1], [2].

One widely adopted approach to securing data in IoT environments is the use of access control frameworks such as Role-Based Access Control (RBAC) [6] and Fine-Grained

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

Access Control [7]. RBAC is a well-established model that assigns access permissions to users based on predefined roles, facilitating manageable access structures within organizations. However, while RBAC offers a structured method for access management, it falls short in IoT environments, particularly in terms of flexibility and scalability.

In large-scale IoT networks where devices and users have diverse and dynamic access requirements, the rigid, role-based permissions of RBAC do not provide the necessary adaptability. Additionally, RBAC's reliance on centralized authority structures introduces single points of failure, limiting its resilience in decentralized IoT environments and raising concerns around both security and operational efficiency.

Fine-Grained Access Control, on the other hand, offers a more precise approach by restricting access based on specific attributes of the user, resource, or environment, allowing for detailed permissions tailored to individual needs [7]. Fine-Grained Access Control attribute-based criteria improve access flexibility, making it a better fit for diverse IoT environments compared to RBAC. However, Fine-Grained Access Control implementations can become complex and computationally intensive as the network size and the number of attributes increase, which can lead to significant scalability challenges. Additionally, Fine-Grained Access Control systems often require continuous updates to access rules, which introduces administrative overhead and potential latency—issues that are problematic in IoT environments where resources and connectivity may be limited.

In contrast, Attribute-Based Encryption (ABE) has emerged as a promising solution to overcome the limitations of RBAC and Fine-Grained Access Control by combining data encryption with access control based on user and resource attributes [8]. ABE's flexibility lies in its ability to encrypt data in such a way that only users with specific attributes, as defined in the access policy, can decrypt the information. This capability provides fine-grained access control without requiring direct management of access rules by a central authority, making it a highly adaptable solution for IoT networks. Moreover, ABE supports the integration of symmetric and asymmetric encryption; symmetric encryption, such as AES, can be used for efficient data encryption, while asymmetric encryption, like RSA or Elliptic Curve Cryptography (ECC), enhances key distribution and management security [9].

Despite these advantages, ABE is not without challenges. Its reliance on complex key management can introduce performance overhead, particularly in environments with frequent attribute updates. Recent research has aimed to reduce this complexity by integrating ABE with blockchain technology, which decentralizes key management and improves scalability. For example, Liu et al. [10] developed a blockchain-assisted ABE framework to address key distribution and user revocation, demonstrating improved resilience and flexibility for IoT applications. This integration addresses ABE's traditional limitations while offering a secure and scalable approach to data protection, aligning closely with the needs of modern IoT systems.

ABE allows for the use of symmetric, asymmetric, and homomorphic encryption, providing robust levels of security. However, it also introduces challenges such as complex key management, performance overhead, and implementation difficulties. In recent years, research has focused on reducing the computational complexity of ABE schemes. For example, Odelu and Kumar Das [9] proposed an ABE scheme that utilizes ECC to reduce key size while maintaining strong security. Their work demonstrated that ECC is an effective tool for creating lightweight cryptographic systems, although there are still trade-offs in terms of decryption time.

In another recent study, Zhang et al. [11] developed a lightweight ABE scheme tailored for edge computing environments. Their approach focused on reducing communication and computation overhead by introducing an optimized attribute revocation process. However, the trade-off in security and efficiency remains a key challenge for these schemes.

Similarly, Du et al. [12] addressed data security challenges in IoT using ABE combined with blockchain technology. Their research showed that integrating blockchain can significantly improve trust and decentralization in IoT networks but highlighted that further scalability optimizations are needed to handle larger networks effectively.

Notably, the work of Das and Namasudra [13] introduced an ABE scheme that utilizes ECC and multiple authorities to enhance security in IoT-enabled healthcare infrastructure. Their approach demonstrated that the use of ECC could significantly reduce key sizes while maintaining high levels of security. However, while such schemes address key size and computational efficiency, there remain challenges in optimizing these solutions for real-world network architectures and ensuring their scalability.

Similarly, Li et al. [14] addressed the issue of computational inefficiency in ABE by introducing decryption outsourcing in IoT environments. Their approach leveraged edge computing to offload decryption tasks, reducing the computational burden on end-user devices. In addition to improving efficiency, their model also tackled key escrow and attribute revocation, enhancing security against collusion attacks.

While these methods offer valuable improvements, there remains a gap in research concerning the integration of blockchain technology into ABE schemes. Blockchain's decentralized and tamper-resistant architecture provides an ideal mechanism for distributed key management and data integrity. However, limited studies have explored how blockchain can be seamlessly integrated into ABE systems, particularly in constrained IoT environments where computational resources are limited. Additionally, guided network architectures and robust feasibility simulations for blockchain-assisted ABE systems are still underdeveloped in current literature.

Liu et al. [10] developed a blockchain-assisted method to tackle key management challenges in ciphertext-policy attribute-based encryption (CP-ABE) systems. Their research addressed significant issues such as key escrow, key distribution, and user revocation through the integration of blockchain technology, which provided decentralized and transparent key management. Notably, they employed a permissioned blockchain and secret-sharing protocols to enhance the security of key generation and distribution. However, their scheme still faced limitations in scalability, particularly in resource-constrained IoT environments, and lacked a robust simulation framework to fully evaluate the system's performance under various network topologies.

Yu et al. [15] focused on enabling attribute revocation in fine-grained access control systems for IoT networks by combining blockchain technology with ABE. Their approach solved the issue of attribute updates, overcoming the incompatibility between blockchain immutability and the dynamic nature of ABE attributes. By incorporating a multilayer blockchain system and Chameleon Hash algorithms, their solution offered a tamper-resistant framework. However, despite these innovations, the lack of in-depth feasibility testing in real-world scenarios, especially in guided network architectures, limits its practical deployment in large-scale IoT systems.

In this work, a comprehensive end-to-end architecture that integrates ABE with Linear Secret Sharing Scheme (LSSS) access policies and blockchain management for secure data transmission in IoT environments. The architecture includes network topology designs and is evaluated using NS3 simulations to assess its feasibility in real-world deployments is present. By combining ECC, ABE, and blockchain technologies, this architecture provides a lightweight, scalable, and secure solution for modern IoT networks. This research aims to expand upon the work done by Das and Namasudra [13] and Yu et al. [15], by providing a robust framework for the network architecture, analysis into different consensus methods, and recommendations for scalability and deployment.

The structure of this paper is organized as follows: Section II provides a comprehensive overview of the cryptographic methods and frameworks employed in this research, including Elliptic Curve Cryptography (ECC), Linear Secret Sharing Scheme (LSSS) access policies, and consensus mechanisms tailored to meet the unique challenges of IoT environments. This section establishes the foundational techniques that address critical gaps in IoT data security, including issues of scalability, lightweight implementation, and decentralized control. Section III presents the proposed system architecture, detailing the integration of Attribute-Based Encryption (ABE) with blockchain to tackle the limitations of traditional encryption methods in ensuring scalable, fine-grained access control and secure key management in IoT. This section also explains how the architecture's decentralized, blockchain-based key management structure mitigates single points of failure and enhances trust across IoT networks. Section IV describes the experimental setup, focusing on the simulated IoT network configurations and the NS3 simulation environment used to evaluate the proposed architecture's performance. The results provide a detailed analysis of metrics such as computational overhead, latency, scalability, and security robustness, demonstrating the practical feasibility and effectiveness of the blockchain-assisted ABE approach. Finally, Section V summarizes the key findings, emphasizing the significance of integrating ABE with blockchain for secure, scalable IoT applications. It also discusses implications for IoT security architecture and suggests future research directions to optimize blockchain-assisted ABE for broader IoT deployments and address remaining challenges in efficiency and real-world implementation.

II. RELATED WORK

A. IOT DATA SECURITY CHALLENGES

The rapid proliferation of IoT devices has introduced new challenges to ensuring data security across distributed networks. IoT environments, which rely on resource-constrained devices to collect and transmit large volumes of sensitive data, face security risks ranging from unauthorized access to data breaches. Traditional cryptographic methods such as symmetric and public-key encryption schemes are often too computationally intensive for IoT devices, prompting the development of lightweight alternatives. Studies such as those by Chen et al. [16] and Kumar et al. [17] emphasize the need for scalable, lightweight encryption techniques that can balance performance with security in large-scale IoT networks. However, many existing solutions struggle to ensure fine-grained access control and suffer from performance bottlenecks, particularly as network size increases. Recent works, such as Zhang et al. [18], continue to explore lightweight cryptography for large-scale IoT, addressing network scalability but with ongoing challenges in dynamic environments.

B. ECC IN IOT SECURITY

Elliptic Curve Cryptography (ECC) has gained widespread attention as a powerful tool for implementing lightweight cryptographic systems, particularly in resource-constrained environments like IoT. The main advantage of ECC over traditional encryption methods, such as RSA, is that it provides the same level of security with much smaller key sizes, thus reducing computational overhead while maintaining strong security guarantees.

Elliptic curves are defined by Equation (1) below.

$$E : y^2 = x^3 + ax + b \pmod{p}, \tag{1}$$

where a, b, x, and y are elements of a finite field F_p, and the curve satisfies the condition $4a^3 + 27b^2 \neq 0$. ECC relies on the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP), which makes it computationally infeasible to derive a private key from the corresponding public key.

In an ECC-based system, a public key Q is generated by multiplying a private key k with a generator point G on the elliptic curve, which can be seen in Equation (2) below.

$$Q = k \cdot G. \tag{2}$$

The security of ECC lies in the difficulty of solving the inverse operation, known as the discrete logarithm problem, where one must compute k given Q and G. This problem is significantly harder than the corresponding problem in RSA for equivalent key sizes, allowing ECC to achieve the same security with shorter keys.

Several researchers have applied ECC to IoT security to address the challenges of resource constraints. Reference [19] demonstrated that using ECC in ABE systems significantly reduces key sizes, making it ideal for IoT devices with limited memory and processing power. Their work built upon foundational concepts of ECC and applied it to IoT-enabled environments, focusing on reducing computational overhead. More recently, Yao et al. [20] explored ECC combined with lightweight authentication protocols for real-time IoT environments, reducing latency while maintaining security.

However, despite its advantages, implementing ECC in ABE schemes presents challenges, particularly in key management and computational efficiency during decryption. [21] introduced the concept of using elliptic curves for cryptography, and subsequent works have explored optimizations for reducing encryption and decryption times. Nonetheless, the trade-off between encryption speed and key size remains an area of active research. Lee et al. [22] have recently developed optimized ECC methods aimed at improving performance in large-scale IoT networks, particularly by balancing computational overhead with security guarantees.

The integration of ECC with blockchain and ABE in IoT environments presents an opportunity to create highly secure and scalable systems. This research builds upon existing works by exploring the full potential of ECC in blockchain-assisted ABE schemes, aiming to provide a lightweight and scalable solution suitable for large-scale IoT deployments.

C. ABE IN IOT SYSTEMS

Attribute-Based Encryption (ABE) has emerged as a promising solution for fine-grained access control in IoT environments, providing a mechanism for securing data based on a set of attributes rather than roles. This flexibility is particularly beneficial in IoT networks, where devices and users often require access to different subsets of data. Bethencourt et al. [8] initially proposed ciphertext-policy ABE (CP-ABE), which has since been widely adopted in IoT for its adaptability. However, the computational complexity and key management issues associated with ABE make it difficult to implement in resource-constrained environments. To address these challenges, researchers like Das and Namasudra [13] have proposed integrating Elliptic Curve Cryptography (ECC) with ABE, significantly reducing key sizes and computational overhead. Recent studies by Zhao et al. [23] have further enhanced the efficiency of ABE systems by introducing hybrid cryptographic schemes tailored for IoT systems. Despite these advancements, practical concerns such as key escrow, attribute revocation, and efficiency in large-scale deployments remain unresolved.

D. BLOCKCHAIN-ENHANCED ABE FOR IOT

The integration of blockchain technology with ABE has gained significant attention for its ability to decentralize key management and enhance trust in IoT environments. Blockchain's immutable and decentralized ledger offers an ideal foundation for managing distributed attributes in ABE schemes without relying on a single trusted authority. Liu et al. [10] developed a blockchain-assisted CP-ABE framework that decentralized key management, tackling issues like key escrow and secure distribution. Liu et al. [25] further expanded on this by enhancing the security and scalability of blockchain-based ABE for IoT data sharing, providing a more robust framework for large-scale IoT environments. While both studies improved security, scalability remains an ongoing challenge, especially in resource-constrained IoT systems.

E. FEASIBILITY TESTING AND SIMULATION FRAMEWORKS

In order to evaluate the practical feasibility of security solutions in IoT environments, simulation tools such as NS2 and NS3 have become essential. These tools provide insights into network performance under various configurations and help validate the scalability of proposed architectures. However, while simulation frameworks are often used to test IoT security protocols, there is limited research that incorporates blockchain-enhanced ABE schemes into these simulations. Sharma et al. [26] used NS2 to test lightweight cryptographic schemes in IoT environments, but their work did not consider the impact of blockchain-based key management systems. Similarly, Ali et al. [27] conducted performance evaluations of ABE in simulated IoT networks, yet their research was confined to traditional ABE models without blockchain integration. Xu et al. [28] extended this area by providing NS3-based simulations for blockchain-assisted IoT, though further exploration into consensus mechanisms is still needed. The work described here aims to fill this gap by conducting comprehensive NS3 simulations to assess the feasibility of a blockchain-assisted ABE system, particularly focusing on network overhead, latency, and scalability.

III. SYSTEM ARCHITECTURE

The system architecture, as illustrated in FIGURE 1 below, is designed to facilitate secure and decentralized data management across a distributed IoT environment. This architecture consists of two primary components: *clients* and *nodes*, each with distinct responsibilities. Clients represent user-end IoT devices, such as sensors, actuators, and smart appliances, that interact with the network by either generating or accessing data. Nodes, on the other hand, represent server-side entities responsible for managing security

protocols, including attribute handling, transaction ordering, and validation [29].

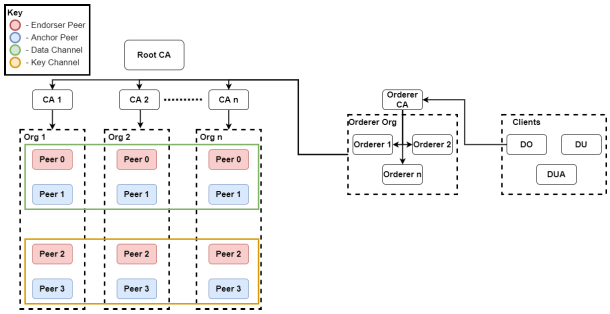

FIGURE 1. Overall system architecture: The system integrates multiple organizations, each managing attributes and facilitating decentralized data and key management.

TABLE 1 provides an overview of the various client roles within the system. Data Owners (DO) are responsible for encrypting and submitting data, while Data Users (DU) are authorized entities that can decrypt specific data based on attribute-based policies. To minimize computational overhead on resource-constrained DUs, Data User Assistants (DUA) support outsourced decryption tasks, enhancing efficiency without compromising data security. These roles reflect the decentralized nature of data management in IoT environments, where different clients have distinct yet interdependent responsibilities [30].

TABLE 1. Client roles and responsibilities.

Client Role	Description
Data Owners (DO)	Responsible for encrypting and submitting data to the system.
Data Users (DU)	Entities authorized to decrypt specific data based on their attributes.
Data User Assistants (DUA)	Assist in outsourced decryption to reduce computational overhead for DUs.

TABLE 2 outlines the key roles of nodes within the system. Each organization in the network includes a Central Authority (CA) for managing root certificates and overseeing high-level network control. Attribute Authorities (AA) are responsible for managing user attributes and generating corresponding keys, ensuring that access control policies are enforced in a decentralized manner. Orderers distribute transactions based on client attributes, Anchor Peers facilitate inter-organizational communication, and Endorser Peers validate transactions according to policy requirements. This structure not only distributes computational tasks but also improves security and fault tolerance by preventing any single point of control [31].

To manage communication between clients and nodes effectively, the architecture employs two dedicated channels, as shown in TABLE 3. The Data Channel handles encrypted data exchanges between nodes, with each organization contributing one anchor peer and one endorser peer to this channel. This configuration ensures that data transactions remain secure and can be validated by multiple peers, enhancing data integrity. Meanwhile, the Key Channel is

TABLE 2. Node roles and responsibilities.

Node Role	Description
Central Authorities (CA)	Manage root certificates and high-level network control.
Attribute Authorities (AA)	Manage user attributes and generate corresponding keys.
Orderers	Distribute transactions based on client attributes.
Anchor Peers	Entry points for inter-organizational communication.
Endorser Peers	Validate and endorse transactions according to policy requirements.

responsible for managing key-related transactions, such as the distribution of encrypted symmetric keys. This separation of communication channels improves efficiency by assigning specific tasks to each channel, reducing network congestion and enhancing overall performance.

TABLE 3. Communication channels.

Channel	Description
Data Channel	Handles encrypted data communication between nodes, involving one anchor peer and one endorser peer from each organization.
Key Channel	Manages key-related transactions such as encrypted symmetric keys. Similarly, each organization contributes peers to this channel.

The operational flow within this architecture begins with clients (DO, DU, or DUA) initiating requests through the orderers, which distribute these requests to relevant peers based on predefined policies. Each organization manages at least one attribute and exercises control over specific data or resources. This decentralized management structure ensures that no single organization holds centralized authority, promoting both security and resilience across the IoT network. By distributing control and decision-making, the architecture mitigates risks associated with centralized failures, which are common in traditional hierarchical systems.

To further enhance scalability, the system dynamically adapts to the growth of attributes in the network. As shown in TABLE 2, each organization manages a subset of up to five attributes. When the number of attributes exceeds 25, a new organization is added to the network, distributing the attribute management load and preventing any single entity from becoming a performance bottleneck [29]. This approach ensures that computational overhead remains balanced across the system, avoiding excessive strain on individual organizations and promoting long-term scalability.

A. MESSAGE ENCRYPTION AND DISTRIBUTION

Each client in the system is assigned a Global Identifier (GID) upon registration with the Root Certificate Authority (CA). The process for generating keys and validating GIDs ensures secure communication between nodes and clients within the network.

When a client registers, it generates a random integer k_n from the order n of the elliptic curve and computes the elliptic curve point R_n using the curve's generator point G, such as in Equation (3).

$$R_n = k_n \cdot G \tag{3}$$

The Root CA generates two random integers α and β, and computes the client's Global Identifier (GID) such as in Equation (4).

$$GID = (device_{ID} + \alpha \cdot \beta \cdot G, \alpha \cdot G) \tag{4}$$

The client's private key is then generated using the client's secret value k_n and the reconstruction parameter λ provided by the CA, such as in Equation (5).

$$Client_{sk} = \text{hash}(C_n) \cdot k_n + \lambda \tag{5}$$

The client uses this private key to compute its public key, such as in Equation (6).

$$Client_{pk} = Client_{sk} \cdot G \tag{6}$$

Once a client has been assigned a GID, they can request a user secret key set (Usk) from the Attribute Authority (AA). The AA generates the secret key Usk based on the client's GID and the AA's secret key, such as in Equation (7).

$$Usk_i = \text{hash}(GID) \cdot AA_{sk_i} + p \tag{7}$$

Additionally, the Data User Assistant (DUA) receives a partial secret key Usk' computed as, such as in Equation (8).

$$Usk'_i = \text{hash}(GID) \cdot AA_{sk_i} \tag{8}$$

To encrypt a message, the Data Owner generates a random symmetric key (csk) and defines an access policy ($\mathcal{A}$, ρ). The secret s and vectors v and u are computed as part of the Linear Secret Sharing Scheme (LSSS) to ensure that only authorized Data Users can decrypt the data. The components C_0, C_1, and C_2 are computed to protect the symmetric key, such as in Equations (9), (10), and (11).

$$C_0 = csk + s \cdot G \tag{9}$$

$$C_1 = \omega_x \cdot G \tag{10}$$

$$C_2 = \lambda_x \cdot G + AA_{sk} \cdot G \tag{11}$$

The Data User can decrypt the message using the parameters N_1 and N_2 computed by the DUA and their own secret key. The ciphertext is decrypted as in Equation (12).

$$csk = C_0 - (N_1 + p \cdot N_2) \tag{12}$$

With the symmetric key csk, the Data User can decrypt the original message.

The overall workflow of the encryption and decryption algorithms can be seen in FIGURE 2 and FIGURE 3 respectively, where n is the number of Attribute Authorities required to manage the number of attributes of the system.

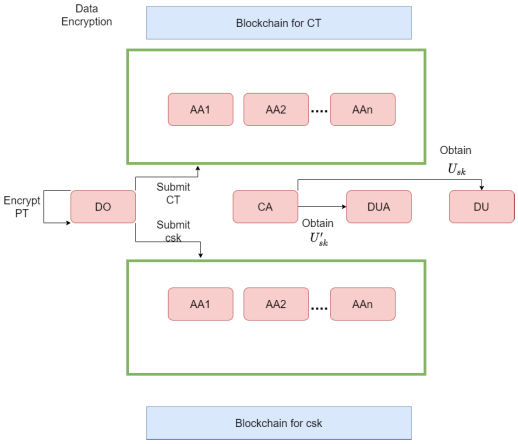

FIGURE 2. Message encryption process: This figure illustrates the secure encryption process involving the Data Owner (DO), where the message is encrypted with a symmetric key and protected by access policies defined through ABE.

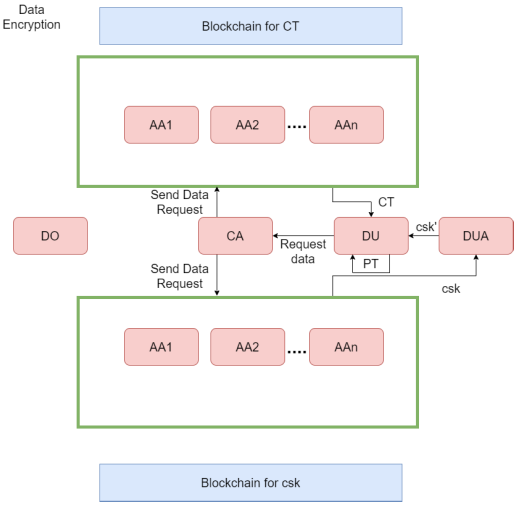

FIGURE 3. Message decryption process: This figure depicts the decryption process handled by the Data User (DU) and Data User Assistant (DUA), where the encrypted message is decrypted based on the user's attributes and the access policy.

IV. RESULTS

A. EXPERIMENTAL ENVIRONMENT

The network simulations were conducted using the NS-3 simulation environment, a discrete-event network simulator commonly used to evaluate network performance. NS-3 was chosen for its flexibility in modeling a wide range of networking protocols and its ability to support custom modules, making it well-suited for testing the performance of the blockchain-assisted Attribute-Based Encryption (ABE) system. Compared to other simulators, NS-3 provides extensive support for layered network simulations and allows for detailed configuration of network parameters, which is essential for evaluating ABE's performance under varied conditions and consensus mechanisms. The choice of NS-3 allows for in-depth assessment of both network-level metrics (such as throughput and delay) and protocol-specific metrics (such as consensus time and encryption performance).

The simulations aimed to evaluate the performance of the proposed system under different network configurations and consensus algorithms, specifically Paxos, Raft, and PBFT (Practical Byzantine Fault Tolerance). Dedicated modules were created in NS-3 to handle each of these consensus algorithms, allowing for comprehensive analysis of their performance under varying network conditions. Parameters such as message size, number of nodes, data rate, and network

delay were varied to assess their impact on consensus time, message overhead, and overall network performance.

B. SIMULATION RESULTS

The results obtained from the NS-3 simulations provided insights into the performance of the Paxos, Raft, and PBFT consensus algorithms and the encryption, decryption, and key generation processes. The performance was measured across several parameters, including message size, number of nodes, data rate, and network delay. This section discusses the results, referencing each plot to illustrate observed trends and insights.

1) CONSENSUS TIME VS DATA RATE

The first set of results examined in this section is consensus time as a function of data rate, and a performance comparison of Paxos, Raft, and PBFT is shown in FIGURE 4 below:

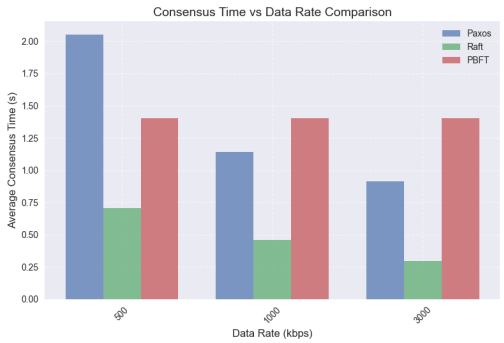

FIGURE 4. Consensus Time as a function of data rate for Paxos, Raft, and PBFT.

As shown in FIGURE 4 above, Paxos is highly sensitive to changes in data rate. At lower data rates, Paxos exhibited a consensus time of over 2 seconds, but this time decreased significantly as the data rate increased, indicating that Paxos may be more suitable for environments with higher data rates. PBFT demonstrated more stable consensus times across all data rates, suggesting robustness to data rate changes, while Raft showed moderate sensitivity, particularly at lower data rates.

2) CONSENSUS TIME VS MESSAGE SIZE

The second set of results evaluated consensus time based on message size, with simulations conducted at 256 bytes and 4096 bytes.

FIGURE 5 above shows that Paxos exhibited the highest sensitivity to larger message sizes, with consensus times rising sharply for 4096-byte messages. Raft and PBFT were more resilient to changes in message size, although PBFT experienced a slight increase in consensus time with larger messages. This suggests that Paxos may be less efficient for systems handling large message sizes, whereas Raft is preferable in scenarios with varying message sizes.

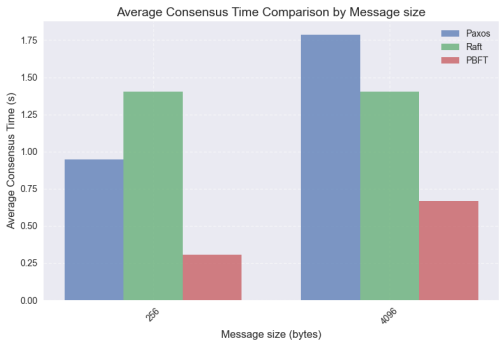

FIGURE 5. Consensus Time as a function of message size for Paxos, Raft, and PBFT.

3) CONSENSUS TIME VS NUMBER OF NODES

The third experiment measured consensus time as a function of the number of nodes, varying from 10 to 30 nodes.

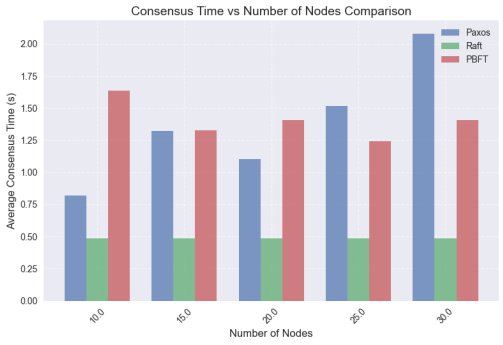

FIGURE 6. Consensus time as a function of number of nodes for Paxos, Raft, and PBFT.

As seen in FIGURE 6 above, Paxos showed fluctuations in response to increasing network size, while Raft demonstrated consistent consensus times across different numbers of nodes. PBFT displayed stability, with no significant change in consensus time as the network size increased. This indicates that Raft and PBFT may be better suited for larger networks, where stability in consensus time is essential.

4) AVERAGE DELAY VS MESSAGE SIZE

Alongside this, simulations also measured the average network delay as a function of message size.

FIGURE 7 above indicates that delay increases significantly with larger message sizes. For 4096-byte messages, the delay reached approximately 0.07 seconds, compared to about 0.04 seconds for 256-byte messages. This highlights the importance of message size in network performance, particularly for consensus protocols with high message exchange rates, like PBFT.

5) AVERAGE THROUGHPUT VS DATA RATE AND NETWORK DELAY

Finally, the throughput was evaluated as a function of data rate and network delay.

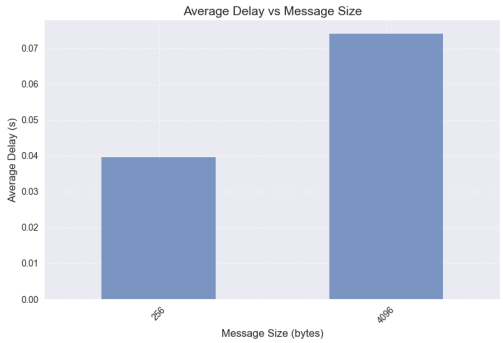

FIGURE 7. Average network delay as a function of message size.

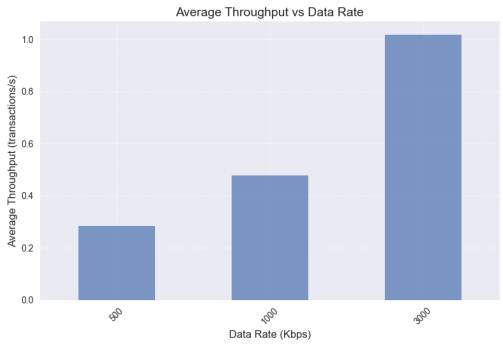

FIGURE 8. Average throughput as a function of data rate.

As shown in FIGURE 8 above, throughput increased with data rate, reaching 1 transaction per second at 3000 kbps. This result emphasizes the relationship between data rate and throughput in high-speed networks. However, FIGURE 9 below shows a significant decline in throughput as delay increased, demonstrating that network delay is a critical factor impacting throughput, with severe throughput reductions observed at 100-second delays.

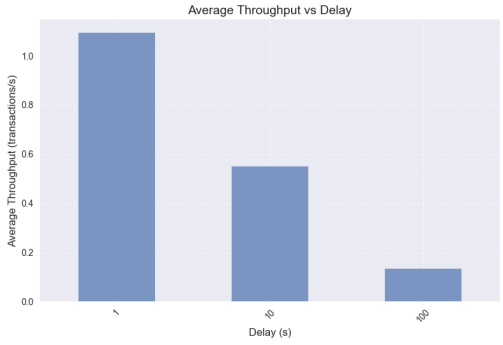

FIGURE 9. Average throughput as a function of network delay.

6) ENCRYPTION, KEY GENERATION, AND DECRYPTION TIMES

In addition to consensus metrics, the performance of the encryption, key generation, and decryption processes was evaluated to provide a complete picture of the ABE system's efficiency. These are critical metrics in understanding the feasibility of the ABE approach for real-time IoT applications.

a: ENCRYPTION TIME

The encryption time was measured as a function of the number of attributes used in the ABE scheme.

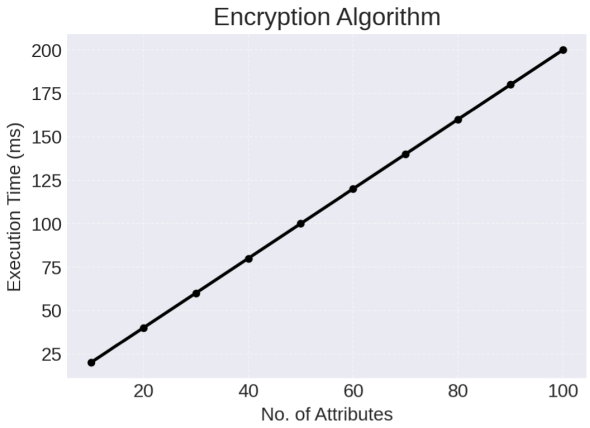

FIGURE 10. Encryption time as a function of number of attributes.

FIGURE 10 above shows that encryption time increases linearly with the number of attributes, reaching approximately 200 ms with 100 attributes. This increase suggests that encryption time could become a bottleneck in scenarios with a high number of attributes, particularly in real-time systems requiring fast response times.

b: KEY GENERATION TIME

Key generation time was also measured as a function of the number of attributes.

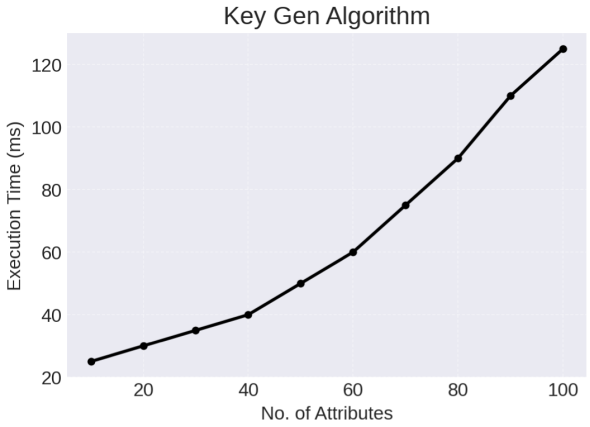

FIGURE 11. Key generation time as a function of number of attributes.

As depicted in FIGURE 11 above, key generation time increases with the number of attributes, although the growth is sub-linear compared to encryption. Key generation time remains below 130 ms even at 100 attributes, indicating that key generation is less of a computational bottleneck than encryption in high-attribute scenarios.

c: DECRYPTION TIME

The decryption time was analyzed to determine its scalability with the number of attributes.

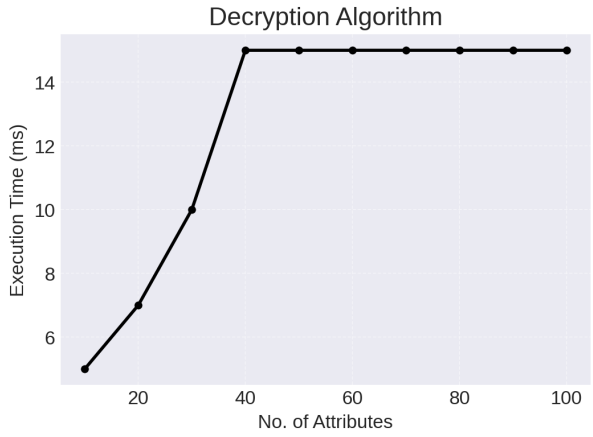

FIGURE 12. Decryption time as a function of number of attributes.

FIGURE 12 above demonstrates that decryption time remains relatively stable as the number of attributes increases, with a minor increase up to approximately 15 ms. This stability in decryption time suggests that the decryption process is efficient and scalable, even in attribute-rich environments, making ABE a viable option for secure and efficient data retrieval in IoT systems.

7) SUMMARY OF FINDINGS

The results indicate that each consensus algorithm offers distinct advantages depending on the network conditions and requirements. Paxos is highly sensitive to data rate and message size, making it suitable for high-speed, low-latency environments. Raft demonstrates resilience across different message sizes and network sizes, indicating its suitability for flexible IoT applications. PBFT, while robust to changes in network size and message size, incurs higher overhead, making it more suitable for applications where Byzantine fault tolerance is critical.

The performance of encryption, key generation, and decryption operations suggests that ABE can support IoT applications with manageable overheads, although the number of attributes directly impacts encryption time. Overall, the ABE scheme, combined with an appropriate consensus protocol, can provide scalable and secure data protection for IoT applications, meeting the varied demands of latency, throughput, and fault tolerance.

8) RECOMMENDATIONS

Based on the results from these simulations, the following recommendations can be made. Raft demonstrated the highest robustness across various network parameters, making it the most suitable algorithm for IoT environments with fluctuating data rates, message sizes, and node counts. PBFT should be deployed in security-sensitive applications where fault tolerance is critical, but it is best suited for smaller message sizes. Paxos, while sensitive to network conditions, can be effective in environments with stable data rates and node counts.

However, all topologies still displayed desirable qualities, as the network architecture allowed Consensus Times as low as 2 seconds in the worst case scenarios and allowed for low delays and high throughput in all scenarios.

V. CONCLUSION

The integration of blockchain technology with Attribute-Based Encryption (ABE) offers a powerful approach to addressing the growing security challenges in modern IoT environments. As IoT networks continue to expand across critical sectors such as healthcare, agriculture, and power generation, the need for secure, scalable, and efficient encryption methods becomes increasingly urgent. This paper presented a comprehensive blockchain-assisted architecture that incorporates ABE with Linear Secret Sharing Scheme (LSSS) access policies and Elliptic Curve Cryptography (ECC) for lightweight, scalable data protection in IoT systems.

Through extensive simulation testing in the NS3 environment, the performance of three consensus algorithms—Paxos, Raft, and PBFT—was evaluated under varying network conditions, including message size, data rate, number of nodes, and network delay. The results demonstrated that Raft provided the most robust performance across different parameters, proving to be highly resilient to changes in data rate, message size, and node count. PBFT, while effective in highly secure environments, exhibited higher sensitivity to message size, making it better suited for applications with smaller payloads. Paxos, although capable of handling fluctuating network conditions, showed greater sensitivity to network size and message size, suggesting that it may be best deployed in stable, well-defined network environments.

The results also revealed that the architecture's ability to scale efficiently through dynamic attribute distribution across multiple organizations mitigates the effects of increasing node count and message size. The architecture's decentralized attribute management ensures balanced computational loads, which maintains network efficiency even as the number of nodes and attributes grows. This system design, combined with the consensus mechanisms evaluated, highlights the potential for achieving both security and scalability in IoT networks while addressing the constraints of computational overhead and delay.

In summary, this research contributes to the body of knowledge by providing a robust, scalable architecture for secure IoT environments. It extends previous work by demonstrating the feasibility of combining ABE and blockchain technology for real-world IoT applications, particularly through the incorporation of ECC and dynamic attribute management. Future work can focus on optimizing this architecture for even larger networks, exploring alternative consensus mechanisms, and conducting further real-world testing to fine-tune performance under various practical constraints. The findings in this paper provide a solid foundation for

future developments in secure, scalable, and efficient IoT data security systems.

REFERENCES

[1] V. Sharma, J. Chen, and A. Kumar, "Security challenges in IoT: A comprehensive survey," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4728–4742, Dec. 2018, doi: 10.1109/JIOT.2018.2855123.
[2] H. Zhang, X. Zhao, and R. Li, "Lightweight encryption schemes for IoT: Recent advances and future directions," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 168–183, 3rd Quart., 2020, doi: 10.1109/COMST.2020.2964741.
[3] X. Chen, L. Li, and P. Wang, "Exploring advanced encryption techniques for IoT security," *IEEE Trans. Industrial Inform.*, vol. 16, no. 2, pp. 1507–1516, Feb. 2020, doi: 10.1109/TII.2019.2927645.
[4] M. Gong, Z. Zhang, D. Zeng, and T. Peng, "Three-dimensional measurement method of four-view stereo vision based on Gaussian process regression," *Sensors*, vol. 19, no. 20, p. 4486, Oct. 2019, doi: 10.3390/s19204486.
[5] A. Lee, B. Park, and C. Lee, "Optimized ECC methods for IoT security," *J. Netw. Comput. Appl.*, vol. 173, Feb. 2021, Art. no. 102860.
[6] C. Xiyuan, W. Di, L. Jian, and Z. Miaoliang, "A security violation detection method for RBAC based interoperation," in *Proc. Int. Conf. Comput. Intell. Secur.*, Guangzhou, China, Nov. 2006, pp. 1491–1496, doi: 10.1109/iccias.2006.295308.
[7] L. Hong-Yue, D. Miao-Lei, and Y. Wei-Dong, "A context-aware fine-grained access control model," in *Proc. Int. Conf. Comput. Sci. Service Syst.*, Nanjing, China, Aug. 2012, pp. 1099–1102, doi: 10.1109/CSSS.2012.278.
[8] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symp. Secur. Privacy*, May 2007, pp. 321–334.
[9] V. Odelu and A. K. Das, "Design of a new CP-ABE with constant-size secret keys for lightweight devices using elliptic curve cryptography," *Secur. Commun. Netw.*, vol. 9, no. 17, pp. 4048–4059, 2016, doi: 10.1002/sec.1587.
[10] S. Liu, J. Yu, L. Chen, and B. Chai, "Blockchain-assisted comprehensive key management in CP-ABE for cloud-stored data," *IEEE Trans. Netw. Service Manage.*, vol. 9, no. 3, pp. 1035–1046, Mar. 2021.
[11] X. Zhang, W. Wang, J. Li, and W. Zhang, "A lightweight attribute-based encryption scheme for secure data sharing in edge computing," *IEEE Access*, vol. 8, pp. 32004–32013, 2020.
[12] L. Du, X. Liu, W. Zhang, and X. Li, "Secure and scalable IoT data sharing scheme based on blockchain-assisted attribute-based encryption," *IEEE Trans. Industrial Inform.*, vol. 17, no. 2, pp. 718–728, Feb. 2021.
[13] S. Das and S. Namasudra, "Multiauthority CP-ABE-based access control model for IoT-enabled healthcare infrastructure," *IEEE Trans. Industrial Informat.*, vol. 19, no. 1, pp. 821–829, Jan. 2023, doi: 10.1109/TII.2022.3167842.
[14] X. Li, T. Liu, C. Chen, Q. Cheng, X. Zhang, and N. Kumar, "A lightweight and verifiable access control scheme with constant size ciphertext in edge-computing-assisted IoT," *IEEE Internet Things J.*, vol. 9, no. 19, pp. 19227–19237, Oct. 2022, doi: 10.1109/JIOT.2022.3165576.
[15] G. Yu, X. Zha, X. Wang, W. Ni, K. Yu, P. Yu, J. A. Zhang, R. P. Liu, and Y. J. Guo, "Enabling attribute revocation for fine-grained access control in blockchain-IoT systems," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1213–1230, Nov. 2020, doi: 10.1109/TEM.2020.2966643.
[16] X. Chen, J. Zhang, Y. Li, X. Liu, and D. He, "A lightweight secure data sharing scheme for cloud-assisted Internet of Things," *Future Gener. Comput. Syst.*, vol. 96, pp. 168–175, Jun. 2020.
[17] R. Kumar, R. Tripathi, and T. Choudhury, "Lightweight cryptographic schemes for IoT devices: A survey," *J. Inf. Secur.*, vol. 10, no. 2, pp. 85–104, 2019.
[18] Z. Zhang, Y. Chen, and J. Li, "A lightweight secure communication scheme in IoT-based smart grids using blockchain and edge computing," *IEEE Access*, vol. 9, pp. 38704–38714, 2021.
[19] L. Liu, Y. Zhang, and X. Li, "Efficient and secure data sharing scheme for IoT devices using elliptic curve cryptography," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 3201–3210, Apr. 2022, doi: 10.1109/JIOT.2021.3112345.
[20] Y. Yao, B. Chen, and L. Xu, "Efficient lightweight authentication and ECC-based key agreement for IoT applications," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 7755–7767, Sep. 2020.
[21] S. V. S. Vasundhara and D. K. V. D. Dr. K. V. Durgaprasad, "Elliptic curve cryptosystems," *Indian J. Appl. Res.*, vol. 4, no. 3, pp. 308–311, Oct. 2011.
[22] H. Lee, K. Kim, and Y. Chung, "Lightweight ECC-based authentication protocol for IoT-enabled smart homes," *IEEE Trans. Consum. Electron.*, vol. 67, no. 1, pp. 93–101, Jan. 2021.
[23] F. Zhao, S. Wang, and Y. Zhang, "Hybrid attribute-based encryption scheme for efficient IoT data security," *IEEE Access*, vol. 8, pp. 116539–116548, 2020.
[24] J. Wang, L. Wu, and X. He, "A scalable blockchain-based CP-ABE system for IoT devices," *IEEE Trans. Industrial Inform.*, vol. 17, no. 6, pp. 4347–4358, Jun. 2021.
[25] P. Liu, Y. Zhang, and X. Wang, "Blockchain-assisted attribute-based encryption with improved security and scalability for IoT data sharing," *IEEE Trans. Industrial Inform.*, vol. 17, no. 10, pp. 6767–6777, Oct. 2021.
[26] P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, "DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 78–85, Sep. 2017.
[27] A. Ali, W. U. Hassan, and S. Hussain, "Performance evaluation of attribute-based encryption in simulated IoT networks," *Int. J. Adv. Comput. Sci. Applications*, vol. 12, no. 1, pp. 456–462, Jan. 2021.
[28] Y. Xu, Y. Zhu, and J. Shen, "Secure and efficient blockchain-enabled IoT network architecture," *IEEE Internet Things J.*, vol. 8, no. 10, pp. 8375–8387, Oct. 2021.
[29] B. Farooq, K. Ali, S. Hussain, and T. Mahmood, "A scalable attribute-based encryption scheme for decentralized IoT networks," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9345–9352, Dec. 2019, doi: 10.1109/JIOT.2019.2939651.
[30] A. Rehman, H. Ali, K. Z. Ghafoor, and A. Salah, "Dynamic attribute-based encryption for scalable IoT applications," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 4, pp. 1568–1581, Apr. 2022, doi: 10.1109/TDSC.2021.3061910.
[31] M. Xie, Y. Zhang, and F. Liu, "Efficient key management and encryption scheme for decentralized IoT networks," *IEEE Access*, vol. 9, pp. 42504–42515, 2021, doi: 10.1109/ACCESS.2021.3066039.

AGUSTIN FERRER-ROJAS was born in Venda, Limpopo, South Africa, in 2000. He received the B.Eng. degree in electronic engineering from the University of Pretoria, in 2024.

BODHASWAR T. MAHARAJ (Senior Member, IEEE) received the Ph.D. degree in engineering in the area of wireless communications from the University of Pretoria. He is a Full Professor and currently holds the research position of SENTECH Chair in broadband wireless multimedia communications (BWMC) with the Department of Electrical, Electronic and Computer Engineering, University of Pretoria. His research interests include OFDM-MIMO systems, massive MIMO, cognitive radio resource allocation, and 5G cognitive radio sensor networks.

MDUDUZI C. HLOPHE was born in Nhlangano, Shiselweni, Eswatini, in 1986. He received the bachelor's degree in electronic engineering from the University of Swaziland, Matsapha, Eswatini, in 2012, and the master's degree in wireless communications from the University of Johannesburg, Johannesburg, South Africa, in 2015. He is currently pursuing the Ph.D. degree in engineering with the University of Pretoria, Pretoria, South Africa. His research interests include mathematical modeling of multivariate statistics, classification methods, knowledge discovery, reasoning with uncertainty and inference, and predictive analytics and inference with applications in wireless communications, finance, health, and robotics.