

Authentication schemes in wireless internet of things sensor networks: a survey and comparison

Pendukeni Phalaagae¹, Adamu Murtala Zungeru¹, Boyce Sigweni¹, Selvaraj Rajalakshmi²

¹Department of Electrical, Computer and Telecommunications Engineering, Botswana International University of Science and Technology, Palapye, Botswana

²Department of Computer Science and Information Systems, Botswana International University of Science and Technology, Palapye, Botswana

Article Info

Article history:

Received Nov 18, 2023

Revised Dec 30, 2023

Accepted Jan 3, 2024

Keywords:

Authentication

Internet of things

Security attacks

Security mechanisms

Wireless sensor networks

ABSTRACT

The proliferation of wireless sensor networks (WSNs) fuels internet of things (IoT's) rapid global development, connecting diverse devices. IoT transforms devices into intelligent entities delivering exceptional services. This work addresses IoT authentication gaps through a comprehensive survey, analyzing recent works and exploring techniques in various applications. It includes a comparative analysis of authentication schemes, evaluating Bi-Phase authentication scheme (BAS) in WSNs. BAS outperforms sensor protocol for information via negotiation (SPIN), broadcast session key protocol (BROSK), and localized encryption and authentication protocol (LEAP), resulting in lower energy consumption and higher efficiency. With energy efficiency at 60 Kb/J for 25 nodes, BAS focuses on power optimization and lightweight security measures, reducing energy consumption, maximizing efficiency, and extending WSN lifespan. The evaluation, conducted using MATLAB/Simulink, demonstrates BAS's superiority, achieving 10 J, 12 J, 14 J, and 15 J energy consumption for 25 nodes during simulation, showcasing its effectiveness and future potential in advancing IoT authentication.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Adamu Murtala Zungeru

Department of Electrical, Computer and Telecommunications Engineering

Botswana International University of Science and Technology

Private Bag 16, BIUST, Palapye, Botswana

Email: zungerum@biust.ac.bw

1. INTRODUCTION

Wireless sensor networks are internet of things (IoT's) backbone, collecting data for applications from smart cities to healthcare. Wireless sensor networks (WSN) consist of a collection of sensors tasked with detecting and monitoring their environment, transmitting data to a central base station for subsequent processing [1]. The IoT is a transformative force, connecting diverse devices that sense, compute, and communicate. However, ensuring IoT security is paramount, given the expansion. IoT security has become increasingly crucial as IoT devices proliferate across various domains, including smart homes, healthcare, industry, and smart cities. According to Garner, Inc., the number of IoT devices will reach 20.4 billion by 2020, driven by the increased adoption of applications such as smart homes, smart cities, and smart healthcare [2]–[5]. The imperative requirement for robust security measures to protect data, mitigate potential threats, and address the challenges posed by widespread technology adoption underscores the critical role of authentication within today's digital landscape.

Authentication is crucial in safeguarding IoT sensor networks by confirming the identities of devices and users, which, in turn, ensures data integrity, device trustworthiness, and user privacy in the IoT ecosystem, thus preserving the reliability and security of data [6]. Authentication in IoT enhances device reliability and user privacy, safeguarding against security risks and intrusion, yet it introduces unique challenges in sensor networks. First, scalability is a primary concern as IoT networks comprise a multitude of devices, requiring authentication methods that can efficiently handle authentication requests at scale [7]. Second, the resource constraints of IoT devices, such as limited processing power, memory, and energy, necessitate authentication solutions that operate efficiently without imposing undue burdens [8]. Finally, the diverse nature of IoT devices, each with varying communication protocols and security requirements, calls for authentication methods that can adapt to this heterogeneity, ensuring interoperability and effective security [9], [10]. Addressing these challenges is essential in developing authentication solutions that effectively secure IoT sensor networks while accommodating the specific demands and limitations of the IoT environment.

In the ever-evolving IoT security landscape, the expanding ecosystem heightens the urgency for robust authentication. Threats, including data breaches, device compromise, eavesdropping, unauthorized access, identity spoofing, and replay attacks, underscore the ongoing challenges in securing interconnected IoT systems and preserving data privacy and confidentiality [11]–[13]. Robust authentication measures are a critical defense line in this evolving landscape, ensuring that only authorized users and devices can access and control IoT systems, safeguarding data integrity, privacy, and overall system security.

This survey is prompted by the increasing importance of robust authentication in sectors such as healthcare, industrial automation, and smart cities. It seeks to thoroughly evaluate and compare existing authentication approaches, providing a valuable resource for researchers, practitioners, and policymakers. By focusing on wireless IoT sensor networks, the survey explores various authentication techniques, protocols, and schemes, conducting a comparative analysis and offering an up-to-date perspective on emerging trends to enhance IoT network security and efficiency.

This article significantly benefits the IoT community, providing a comprehensive view of authentication in wireless IoT sensor networks, evaluating existing schemes, and offering insights into emerging trends. It empowers informed decision-making, enhances security, and drives innovation in IoT, serving as a valuable resource for both professionals and researchers in this field. The contributions of this work are:

- A comprehensive review and classification of recent works on IoT authentication schemes and analysis on the strength, weakness, and uniqueness of the survey.
- A review on Applications, emphasizing on their authentication techniques, accounting for their suitability for diverse IoT use cases.
- A comparative analysis of existing authentication schemes, highlighting their methods, strengths, weaknesses and analyzing their performance based on energy efficiency, secure key management, scalability, robust security, and resistance to attacks.
- Simulation and analysis of authentication schemes in IoT including evaluating the effectiveness of the BAS in comparison to other cryptographic-based authentication schemes in WSNs, namely SPIN, broadcast session key protocol (BROSK), and localized encryption and authentication protocol (LEAP).
- Identification and highlight of emerging trends and innovations in IoT authentication to offer insights into the future of authentication in IoT sensor networks.

The remaining sections of the paper are organized as follows: the second section examines similar efforts, while the third section presents an overview of authentication in WSN, the fourth section covers authentication schemes associated the IoT. The fifth section presents experimental results and performance evaluation of authentication schemes in IoT based wireless sensor networks. The sixth section, concludes the work and discusses future trends in providing security solutions.

2. RELATED WORKS

In recent years, researchers have conducted extensive investigations into authentication solutions for wireless IoT sensor networks, with a specific focus on the recent developments in IoT authentication. Table 1 presents a detailed comparison table on recent works in IoT authentication, systematically reviewed for strengths, weaknesses, and future research directions. Contributions include a comprehensive exploration of IoT authentication techniques [14], an investigation of communication protocols for IoT security [15], and a taxonomy tracing the evolution of IoT authentication methods [16]. Kavianpour *et al.* [17] provides a thorough analysis of IoT authentication, encompassing security aspects and identifying future challenges. Surveys by Singh *et al.* [18] and Bahache *et al.* [19] explore user authentication schemes for WSNs and authentication in wireless medical sensor networks (WMSNs) for healthcare respectively. Gautam and

Kumar [20] evaluate WMSN authentication schemes, offering a comprehensive review and future research directions. The work presented by Wang *et al.* [21] classifies authentication methods, evaluating usability and security, and examines mobile device authentication.

In summary, diverse surveys on IoT authentication solutions offer comprehensive insights, exhibiting strengths like thorough exploration and innovative taxonomies. While providing valuable overviews, areas for improvement include offering more specific technical details and real-world examples. Nevertheless, collectively, these surveys contribute significantly to understanding authentication in wireless IoT sensor networks and guide future research.

3. OVERVIEW OF AUTHENTICATION IN WSN

The surge in IoT device numbers has led to heightened security and privacy challenges, including threats like man-in-the-middle attacks and data breaches. Authentication of connected devices is essential, addressing privacy concerns by ensuring data confidentiality and privacy within the network [22]. It plays a critical role in communication security by verifying the legitimacy of data sources, confirming the accuracy and authorization of information exchanged between network nodes.

3.1. Authentication scenarios

In WSNs, there are two authentication scenarios: pairwise and groupwise. Figure 1 demonstrates authentication scenarios in IoT Figure 1(a) illustrates pairwise authentication between nodes x and y. Group-based authentication includes cluster-based authentication and global-based authentication [23]. A cluster head and its nearby sensor nodes use cluster-based authentication, as shown in Figure 1(b), to secure clustered broadcast messages. Node authentication, as shown in Figure 1(c), is validated by the manager node and all sensor nodes in the sense field. The manager node performs global authentication to secure communications broadcast to the whole network and prevent unauthorized sensor nodes from joining the network.

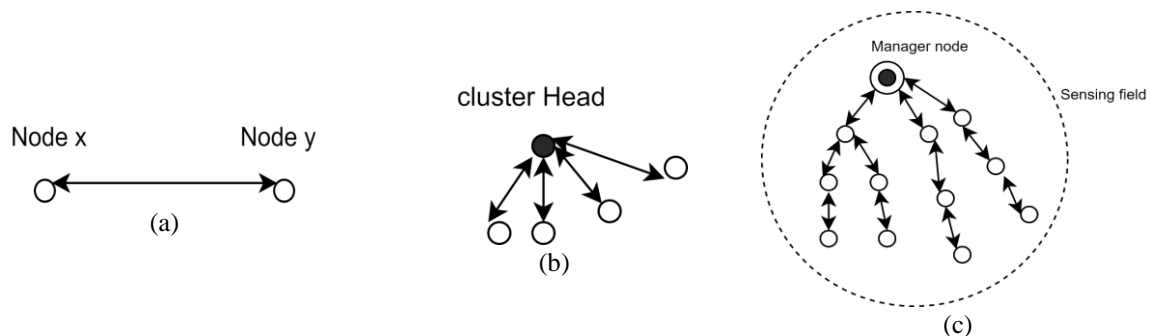


Figure 1. Authentication scenarios in IoT: (a) pairwise authentication, (b) cluster authentication, and (c) group-wise authentication

3.2. IoT device authentication techniques

To enhance security measures for devices and networks within IoT-based WSNs, a variety of authentication systems can be employed. The choice of an authentication scheme is contingent upon the specific security requirements of the IoT-based WSN and the available resources on both devices and the network [24]. Among the widely adopted authentication schemes in IoT-based WSNs are:

3.2.1. Pre-shared key

For authentication, a shared secret key is disseminated among all devices and the network in this system. When a device wants to join the network, it needs to provide the correct shared secret key for authentication. In most IoT wireless networks, the authentication process involves pre-configuring a newly joining node with a pre-shared key (PSK) in the initial authentication phase. Each device, possessing a distinctive identifier, must pre-share a symmetric key with the network coordinator which allows the network coordinator to authenticate recognized devices when engaging in subsequent communications [25]. However, IoT networks lack a well-defined procedure for sharing pre shared keys.

Table 1. Recent works on IoT authentication

Title	Citation	Description	Strength	Weakness	Uniqueness of work
A survey of I IoT authentication schemes	El-Hajj <i>et al.</i> [14]	Comprehensive IoT authentication review with a dedicated taxonomy.	In-depth IoT authentication taxonomy, multi-criteria classification, and protocol analysis.	Lacks specific solutions or protocols to address these issues.	Thorough analysis of IoT authentication, hardware security trends, sets it apart as forward-thinking.
Key agreement and authentication protocols in the IoT: a survey	Szymoniak and Kesar [15]	Explores security protocols for IoT and WSNs, including new solutions.	Examines IoT and WSN security, focusing on critical aspects like anonymity, common attack types, and protective measures.	Lacks specific solutions or protocols, limited exploration of cross-platform compatibility and use cases.	Highlights efficient tech like elliptic curves and biometrics, with a focus on future secure communication research.
A comprehensive survey of authentication methods in IoT conjunctions	Kumar <i>et al.</i> [16]	Analyzes IoT authentication, security, evolution of solutions, and research challenges.	Evaluates IoT authentication across domains, highlights challenges, future research.	lacks specific technical details or practical implementation examples.	Comprehensive analysis of IoT authentication, its taxonomy across domains.
A systematic literature review of authentication in IoT for heterogeneous devices	Kavianpour <i>et al.</i> [17]	Analyzes diverse IoT authentication methods: cloud-based, lightweight, decentralized blockchain-based, and biometrics-based.	Extensively examines IoT authentication challenges, various methods, security aspects, and formal verification.	Does not present precise solutions or elaborate strategies to overcome these limitations.	Presents various authentication methods and formal verification tools and the ongoing need for IoT authentication improvements as a future research area.
Evaluating authentication schemes for real-time data in wireless sensor network	Singh <i>et al.</i> [18]	Categorizes and evaluates user authentication schemes for WSNs based on: security, efficiency, communication, and computation costs	Systematic evaluation framework, extensive scheme categorization, and the call for improved authentication methods	Does not propose new authentication schemes, leaving room for further research.	Detailed analysis and the model-based evaluation of authentication schemes for WSNs, providing valuable insights for future research and development.
Authentication schemes for healthcare applications using wireless Medical sensor networks: a survey	Bahache <i>et al.</i> [19]	Evaluates WMSN authentication schemes by architecture, assessing security, performance, and exploring attacks and verification.	Comprehensive review, experiments, and future research directions for enhanced WMSNs authentication schemes.	Focus on WMSNs authentication may limit its relevance to broader IoT applications.	Analyzes healthcare and IoT security authentication, emphasizing tailored solutions for resource constraints like WMSNs, backed by practical experiments.
A comprehensive study on key management, authentication, and trust management techniques in wireless sensor networks	Gautam and Kumar [20]	Classified authentication schemes and evaluated them based on key network security aspects, including resource efficiency and strong security.	Emphasizing reduced computing load, lower energy consumption, high security, and efficient resource utilization in various authentication schemes.	The paper is deficient in terms of specific technical intricacies and practical implementation illustrations.	Categorizes authentication schemes, evaluates them based on network security, providing a unique perspective for enhanced understanding and comparison.
User authentication on mobile devices: approaches, threats, and trends	Wang <i>et al.</i> [21]	Classifies authentication into knowledge-based, physiological and behavioral biometrics, two/multi-factor authentication. Evaluates usability and security	Comprehensive analysis of mobile device authentication, noting strengths/weaknesses and emphasizing the emerging trend of multi-factor authentication.	insufficient coverage on emerging mobile authentication technologies, lacks a clear solution for the usability-security trade-off.	Categorizes and assesses trends in mobile device authentication, exploring integrated metrics for enhanced security and user convenience, with implications for future research.

To address the challenge of undefined procedures for sharing PSK in IoT networks in large-scale and dynamic environments like industrial IoT (IIoT), Haj-Hassan *et al.* [26] introduces an autonomous mutual authentication and key establishment protocol, providing a systematic approach to PSK sharing. Through certificate-based authentication and a lightweight consensus mechanism, the protocol enhances security and efficiency in large-scale IIoT networks where traditional standards lack clarity.

3.2.2. Certificate-based

This scheme uses digital certificates to authenticate devices and the network. Each device has a unique digital certificate that is signed by a trusted certificate authority (CA). When a device wants to join the network, it presents its digital certificate to the network for authentication [27]. The work presented by Khurshid and Raza [28] proposed an integrity certificate-based authentication scheme to address IoT security challenges by proposing automated certification for IoT (AutoCert), a novel time-of-check to time-of-use (TOCTOU)-secure mechanism combining software-state integrity with public key infrastructure (PKI) for device authentication. AutoCert, implementing internet engineering task force (IETF) remote attestation procedures and X509 IoT certificates, resolves the TOCTOU problem in integrity certificates. The proof-of-concept on a real IoT device, the OPTIGA trusted platform module (TPM) evaluation kit, demonstrates practicality, achieving attested state validation in approximately 4,746 milliseconds with minimal network overhead.

3.2.3. Biometric based

This scheme uses biometric features such as fingerprints, facial recognition, or iris scans for device authentication [29]. Biometric-based authentication is more secure than other authentication schemes as biometric features are unique to everyone. The work proposed by Mirsarai *et al.* [30] introduces a three-factor authentication scheme for IoT on a blockchain platform. It offers mutual authentication with user authorization through smart card registration on a private blockchain, eliminating the need for a trusted server. Utilizing elliptic-curve cryptography (ECC) and rigorous security analysis, this approach enhances security and computational efficiency in IoT environments. It introduces a biometrics-based authentication method, striking a balance between robust security, privacy preservation, and reduced computational resource consumption.

3.2.4. One-time password

For each authentication session, this scheme generates a unique password. The password is only good for one authentication session and cannot be used again. This scheme is commonly used for online banking and other financial transactions. The work presented by Kaur *et al.* [31] suggests a two-factor authentication scheme to bolster security and privacy in cloud computing, targeting challenges and vulnerabilities in cloud communication amid its pervasive adoption in reshaping information technology (IT) and business operations. The proposed authentication scheme combines traditional user credentials, one-time passwords (OTP), one-way hash, and nonce-based techniques to counter various attacks, reinforcing user authentication and ensuring secure access to cloud services for overall security in the cloud ecosystem.

3.2.5. Token-based

A token is produced for each authentication session under this scheme. The token is used to validate the device and user's identities [32]. This scheme is commonly used for multi-factor authentication. The work presented by Jiang *et al.* [33] introduces EdgeAuth, a novel token-based authentication scheme designed for rapid user authentication in edge computing environment. EdgeAuth improves authentication efficiency in Industrial IoT by leveraging cloud-edge collaboration. The authentication process, starting with cloud verification and followed by edge server validation enhances speed and security, effectively countering common authentication attacks and presenting a significant advancement for geographically distributed edge servers.

3.2.6. Public key infrastructure

The described scheme employs a public-private key pair for authentication in IoT devices. Yang *et al.* [34] introduced as an interaction-based authentication (IBA) scheme, it addresses security and efficiency challenges in IoT networks. IBA utilizes device characteristics from previous interactions to securely authenticate through element matching, eliminating the need for a constant connection to trusted third parties. The scheme exhibits dynamic adaptability, scalability, and resilience against common attacks like replay, impersonation, and man-in-the-middle attacks. Comparative analyses indicate that IBA outperforms existing authentication schemes in terms of security and performance, making it a more practical solution for IoT environments.

3.3. Use cases and industry application of authentication in IoT

Authentication is crucial in diverse IoT applications, encompassing smart homes, connected healthcare, industrial IoT, smart cities, energy grid management, supply chain management, smart agriculture, connected vehicles, smart retail, and environmental monitoring [35]. Applications in diverse sectors utilize various authentication techniques for IoT security. Examples include smart home security

employing biometric and secure communication for residential safety, industrial IoT relying on certificate-based authentication for machinery protection, and smart cities ensuring secure IoT devices through communication encryption. Other applications span healthcare data security, energy grid management with mutual authentication, supply chain transparency via blockchain, and smart agriculture protecting data integrity. Connected vehicles use biometric and key management, while smart retail emphasizes secure payment gateways. Environmental monitoring safeguards data integrity and access control in ecological research.

3.4. Challenges in IoT authentication

Authentication in the IoT encounters a myriad of challenges, necessitating solutions for effective operation. These challenges encompass resource limitations, scalability issues, diverse devices, intermittent connectivity, key management complexities, physical security concerns, privacy considerations, update processes, vulnerabilities, and adherence to standards, energy efficiency, and integration with edge computing, and compliance with regulations. Addressing these multifaceted challenges is imperative to establish a robust and secure framework for IoT authentication. Some specific challenges in IoT authentication include:

- Resource constraints: limited processing, memory, and energy resources in IoT devices challenge the implementation of robust authentication, as traditional methods can be computationally intensive and overburden these devices.
- Scalability: IoT networks can comprise a massive number of devices, from sensors to actuators. Ensuring efficient and scalable authentication methods becomes crucial to handle authentication requests from this vast device population without causing network congestion or overwhelming authentication servers.
- Heterogeneity: IoT ecosystems encompass a wide range of devices with diverse capabilities, communication protocols, and architectures. Authentication solutions need to be adaptable to this heterogeneity and ensure interoperability across the varied devices and platforms.
- Secure key management: IoT devices often rely on cryptographic keys for authentication and secure communication. The challenge lies in securely managing these keys across many devices. Key distribution, secure storage, and timely revocation of compromised keys must be carefully managed to maintain security.
- Physical security: IoT devices are often deployed in physically exposed environments, making them susceptible to tampering and physical attacks. Ensuring the physical security of authentication mechanisms is essential to prevent unauthorized access or manipulation of devices.
- Privacy concerns: IoT devices often collect sensitive data, and authentication solutions must consider privacy concerns. It is imperative that user data is protected and only accessible to authorized entities, addressing privacy regulations and user expectations.
- Energy efficiency: many IoT devices operate on battery power, making energy-efficient authentication essential to extend device lifespans. Traditional authentication methods, which may consume significant energy, pose challenges in meeting the energy constraints of IoT devices.

3.5. Authentication requirements

Authentication in IoT sensor networks is vital to meet stringent requirements, ensuring robust network security, data integrity, and overall reliability. The fulfillment of these requirements becomes indispensable for safeguarding critical data, securing devices, and maintaining the integrity of the entire IoT sensor network [36]. The authentication process plays a pivotal role in establishing trust and preventing unauthorized access, contributing to the overall resilience and dependability of the IoT sensor network.

- Scalability: IoT sensor networks often comprise many devices, necessitating authentication solutions that efficiently handle the scaling requirements without causing network congestion or delays.
- Resource efficiency: authentication mechanisms for IoT sensors must efficiently operate on resource-constrained devices with limited processing power and memory, minimizing resource consumption.
- Memory usage: the amount of memory required by the algorithm can impact the performance of the system. Algorithms that require less memory may be more efficient and faster.
- Low energy consumption: energy-efficient authentication is crucial for IoT sensors running on battery power, extending operational lifespan, and reducing the need for frequent battery replacements.
- Robust security: authentication is the primary defense for securing IoT sensor networks, ensuring robust protection against unauthorized access, data tampering, and eavesdropping to maintain data integrity and privacy.
- Authentication methods diversity: authentication solutions should offer flexibility to support a range of methods, including certificates, biometrics, and tokens, to accommodate different sensor types.

- Resilience to physical attacks: IoT sensors are often physically exposed, making them susceptible to tampering or theft. Authentication mechanisms should be designed to resist physical attacks and protect sensitive credentials.
- Secure key management: proper key management is fundamental to authentication in IoT. It ensures the secure storage, distribution, and revocation of cryptographic keys, preventing key compromise and misuse.
- Key size: the key size in an algorithm impacts both security and encryption speed. Larger key sizes generally offer higher security levels but can also increase the time needed for encryption and decryption.
- Privacy preservation: IoT sensors often handle sensitive data. Authentication solutions must prioritize user and data privacy, ensuring that only authorized entities can access and process this information.

3.6. Security threats and vulnerabilities in IoT authentication

In IoT authentication, there is a critical focus on addressing an array of security threats and vulnerabilities. These encompass concerns such as brute force attacks, password cracking, phishing, man-in-the-middle attacks, credential theft, session hijacking, and replay attacks. Effectively mitigating these threats is imperative to uphold the integrity of authentication security and ensure the safeguarding of sensitive data in various systems and applications.

- Brute force attacks: systematic trial-and-error attempts to guess credentials, particularly problematic with weak passwords.
- Password cracking: exploiting stored password weaknesses through techniques like dictionary attacks or rainbow tables.
- Phishing: deceptive attempts to acquire user credentials by impersonating trusted entities or services.
- Man-in-the-middle attacks (MitM): intercepting communication between user and authentication server, enabling eavesdropping or impersonation.
- Credential theft: stealing passwords, tokens, or keys via malware, social engineering, or exploiting authentication vulnerabilities.
- Session hijacking: unauthorized access by acquiring session tokens, posing as the legitimate user.
- Replay Attacks: Capturing authentication data and replaying it to gain unauthorized access.
- Weak encryption: insufficiently protected authentication data can expose credentials to eavesdroppers.
- Single points of failure: relying solely on one authentication factor (e.g., passwords) is risky; implementing multi-factor authentication (MFA) is more secure.
- Insufficient user authentication: weak or improper validation of user identities may lead to unauthorized access.
- Biometric spoofing: vulnerabilities in biometric authentication where attackers can mimic biometric data to gain unauthorized entry.
- Cross-site scripting (XSS): malicious code injections in web applications can capture authentication data, threatening user credentials.
- Software vulnerabilities: flaws in authentication software or libraries can be exploited, jeopardizing security.
- Social engineering: manipulating user psychology to divulge authentication information or reset passwords, exploiting human rather than technical vulnerabilities.
- Token leakage: unauthorized access due to token leaks through insecure storage or communication channels.

4. AUTHENTICATION SCHEMES IN IOT

In the following sub-sections, the paper delves into various authentication schemes employed in the context of the IoT. These schemes encompass a range of approaches such as identity (ID)-based, broadcast, timestamp, and cryptographic-based authentication, each of which is categorized to facilitate a thorough analysis. The exploration and discussion of these diverse authentication modes contribute to a comprehensive understanding of their applicability and effectiveness in IoT environments.

4.1. Identity-based authentication

This authentication method is crucial for diverse applications, providing security against various risks in networks like mobile ad hoc, automotive, grid, smart cards, and wireless sensor networks (WSNs). It employs certificateless cryptography to address ID-based authentication challenges, including key escrow and certification issues. A proposed conditional preservation of authenticity enhances resilience by implementing a secure authentication system between the base station and sensor nodes, designating a cluster

leader, and assigning unique identities to member nodes [37]. The protocols, incorporating key distribution and secure data transmission components, also guard against random oracle and quantum computer attacks. Additionally, Deebak *et al.* [38] introduces an ID-based authentication mechanism using lattice and rejection sampling from number theory.

4.2. Broadcast authentication

Broadcast authentication is valuable in remote settings, requiring low compute overhead, instant verification, time synchronization, and defense against security concerns. There are two categories of broadcast authentication, signature and timed, efficient, streaming, loss-tolerant authentication (TESLA) authentication. Signature authentication uses cryptographic primitives and henceforth faces challenges like larger key sizes. The efficient identity-based broadcast authentication scheme (EIBAS) aims to protect multiple nodes without a mobile base station, involving system initialization, cryptographic key mining, signature creation, and broadcast authentication [39]. The lightweight one-way cryptographic hash algorithm (LOCHA) translates messages into American standard code for information interchange (ASCII), reducing storage and transmission overhead [40]. Another signature-based approach divides messages into blocks, each authenticated by a previous authenticator, providing high-security levels without requiring time synchronization [41].

4.3. Time stamp-based authentication

The authentication method employs a public and private key pair, with each device having a distinct public key. A trust-based security mechanism in WSNs uses linked chained authentication, incorporating load and header into a block [42]. The authority generates a payload with public key and cryptographic information for each added sensor node. The payload assesses block credential validity using the trust credit score. The mobile ad hoc network's authentication approach validates messages using a timestamp and ECC-based encryption, offering mutual authentication based on time synchronization. This method, demonstrated using bloom filters and the hybrid certification scheme (HAS), ensures secure secret and session keys, guarding against tracking attacks, data leaks, and identity theft. Mobility challenges in wireless sensor networks prompt frequent re-authentication.

The work presented by Chunka *et al.* [43] critiques password and key-based authentication, advocating for biometric data use. The author demonstrates biometric authentication's superiority, being challenging to copy, guess, steal, lose, disperse, or forget. A timestamp cryptographic algorithm aids in jamming attack defense. Xu *et al.* [44] introduce creating a new sensor node cluster and generating timestamps between nodes. The receiver's end calculates the timestamp value, discarding messages with significant timestamp discrepancies, indicating malicious intent. Despite its simplicity, this algorithm produces effective results. The work presented by Sankar *et al.* [45] proposed a localized encryption and authentication protocol utilizing four keys: individual, pairwise, cluster, and group keys. The scheme authenticates broadcasted data packets and addresses key revocation.

4.4. Cryptographic-based authentication

Cryptographic methods secure data in communication systems like messaging apps and online transactions use mathematical algorithms to secure data in communication systems. Maurya *et al.* [46] introduces the BAS for WSN, emphasizing lightweight security, minimal energy consumption, and resistance to denial-of-service attacks. BAS enables external authentication for WSN users, employing shared and paired keys, and each node possesses a pairwise shared key with the base station. Despite its resilience to denial of service (DoS) attacks and minimized energy consumption, BAS is vulnerable to tamper attacks and lacks internal network security features, such as ensuring data integrity, freshness, and confidentiality.

Qazi *et al.* [47] introduces a localized encryption and authentication protocol addressing key revocation and ensuring lightweight encryption within the network. It employs various key types for authenticating base station broadcasts, data packets, and supporting key revocation. While effective in secure key management and protection against eavesdropping attacks, the protocol is criticized for its energy inefficiency, lack of scalability, and vulnerability to DoS and tamper attacks.

Gaur [48] present the SPINs, incorporating sensor network encryption protocol (SNEP) for data confidentiality and authentication, and micro timed, efficient, streaming, loss-tolerant (μ TESLA) for authenticated broadcast in resource-constrained environments. The protocol utilizes a key distribution center (KDC) to ensure data confidentiality, offering advantages such as confidentiality, two-party data authentication, data integrity, and freshness. SPIN demonstrates energy efficiency, secure key management, and defense against DoS attacks. However, it faces challenges in scalability and is vulnerable to issues like DoS attacks, eavesdropping, and tampering.

Vandervelden *et al.* [49] introduce the BROS, a broadcast negotiation protocol that eliminates the requirement for a trust server and showcases scalability and energy efficiency when compared to SPIN. This

protocol employs a secure communication protocol for broadcasting in WSNs through negotiation. In BROS, every node shares a common master key, and nodes use their keys to validate other nodes. While BROS is highly scalable and provides secure key management, it lacks energy efficiency and is susceptible to DoS, eavesdropping, and tamper attacks.

Zhang *et al.* [50] addresses security concerns in WSNs through the introduction of a novel encryption scheme that combines ECC and homomorphic encryption. Homomorphic encryption is intentionally designed to allow computations on encrypted data without the requirement for prior decryption, thereby strengthening privacy and providing effective protection against eavesdropping. The scheme's weaknesses lie in the potential energy consumption from computational complexity, susceptibility to DoS attacks, and the need to ensure robust protection against tamper attacks. Implementing measures such as access control and intrusion detection is vital to augment the security of these cryptographic authentication methods. This involves considering the strengths and weaknesses inherent in each authentication scheme.

5. RESULTS AND DISCUSSION

This section assesses the effectiveness of cryptographic authentication schemes and presents the experimental results. The results are generated using MATLAB/Simulink software, which produces both graphical and numerical analyses. The experiment involves randomly distributing sensor nodes within a 16 m × 16 m rectangular area. Table 2 delineates the simulation parameters, encompassing network size, node quantity, energy consumption, sink node placement, and packet size.

Table 2. Simulation parameters

Parameters	Values
Type of simulation	MATLAB
Standard	IEEE 802.11
Simulation time	100s
Energy	25J
Number of nodes	100
Size of network	16 m×16 m
Energy	10J
Position of sink node	(10, 10)
Packet size	6,400 bits

5.1. Simulation metrics

To assess the effectiveness of an authentication strategy, performance measures for cryptographic authentication are utilized. The following are some of the key performance metrics for cryptographic authentication schemes. The effectiveness of BAS in comparison to other cryptographic based authentication schemes in WSNs; SPIN, BROS, and LEAP was evaluated. For comparisons between the procedures, the performance metrics below are noted:

Energy consumption: defines the total power consumed by nodes in the network measured in joules. Energy consumption is the measure of how much energy the authentication method uses. Energy consumption is particularly important in battery-powered devices, where energy conservation is critical. Encryption and decryptions are computationally expensive and consume more power. In (1) and (2) evaluate the overall transmission energy. The calculation of the overall message's transmission energy TT_E and reception energy R_E involves the consideration of both the transmitting energy T_E , receiving energy R_X as well as the number of transmitted packets S_p and the distance traveled D .

$$TT_E = T_E(S_p, D) \quad (1)$$

$$R_E = R_X(S_p) \quad (2)$$

The calculation of the total energy consumed, denoted as E_T , is determined through the application of (3).

$$E_T = TT_E + R_E \quad (3)$$

Where TT_E , presents the transmission energy and R_E presents the receiving energy. Energy efficiency (EE): a measure of packet transmission to the BS in relation to the overall energy consumed by the SNs measured in (kb/J) calculated by (4).

$$EE = (E_T - \frac{TT_E}{E_T} * 100) \tag{4}$$

5.2. Simulation results

5.2.1. Energy consumption

The BAS outperforms SPIN, LEAP, and BROSK in reducing power usage in WSNs through its multi-hop routing approach, utilizing a two-factor authentication process. SPIN consumes less energy due to its negotiation mechanism, while BROSK excels as the most energy-efficient by broadcasting a session key. LEAP, focused on data confidentiality through encryption algorithms, consumes more power. Understanding the energy consumption of these protocols is crucial for selecting the most suitable one in energy-constrained environments. Figure 2 demonstrates that BAS outperforms SPIN, LEAP, and BROSK in reducing power consumption.

5.2.2. Energy efficiency

A network is expected to perform optimally without performance degradation despite an increase in network devices. Figure 3 analyzes energy efficiency of BAS, SPIN, BROSK and LEAP. Figure 3 illustrates that BAS excels in maximizing energy efficiency compared to SPIN, LEAP, and BROSK. It is evident from the results that BAS maximizes energy efficiency by 97% as compared to other protocols in consideration. These results correspond to low energy consumption of the protocols as discussed in Figure 2. Using a multi-hop routing strategy has a substantial influence on lowering overall energy usage, enhancing energy efficiency when the distance cost is considered.

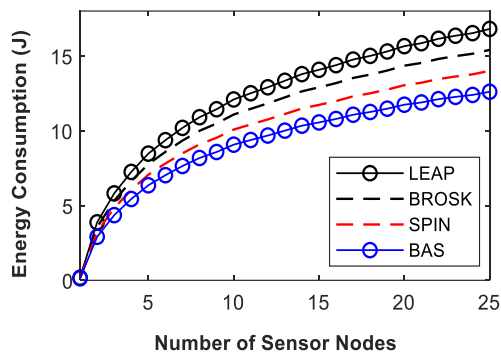


Figure 2. Energy consumption with respect to number of nodes

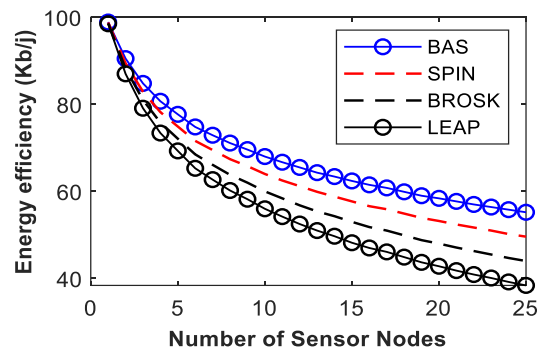


Figure 3. Energy efficiency with respect to number of nodes

6. CONCLUSION

IoT has experienced significant growth due to wireless sensor networks, offering benefits such as intelligent devices and transformed environments. Despite ongoing efforts to address security concerns in the IoT, research gaps remain. These gaps include the necessity for thorough reviews and classifications of recent studies, detailed comparisons of security attacks and cryptographic schemes, examination and categorization of authentication methods, and assessments of encryption-based authentication protocols. This work significantly contributes to IoT authentication through a comprehensive review and classification of recent works, emphasizing strengths, weaknesses, and uniqueness. It extends its impact by reviewing applications, assessing their authentication techniques for diverse IoT use cases, and conducting a comparative analysis of existing authentication schemes, considering key metrics. The study includes a simulation and analysis, evaluating the effectiveness of the BAS against other cryptographic-based authentication schemes. Additionally, the work identifies emerging trends, offering insights into the future of IoT authentication in sensor networks. Exploring emerging trends and innovations in IoT authentication is crucial for maintaining the security and efficiency of IoT systems. Examining advanced biometric methods such as vein pattern recognition, improving algorithms for behavioral authentication, and incorporating passwordless approaches with quantum-resistant cryptographic keys can bolster security. Furthermore, exploring blockchain for decentralized authentication records, implementing homomorphic encryption for privacy in IoT, establishing standardized and lightweight authentication protocols for IoT, researching cross-domain authentication, and assessing the impact of emerging technologies like artificial intelligence (AI) and sixth generation (6G) networks on authentication are crucial areas of study. This through examination of

future directions aims to assist researchers and practitioners in navigating the evolving challenges and opportunities in IoT authentication.

ACKNOWLEDGMENTS

The Botswana International University of Science and Technology deserves credit for provision of funding and resources employed to make this study a success. Also, a special thanks to the Department of Electrical, Computer, and Telecommunications for their inspiration and assistance.




REFERENCES

- [1] N. Al-Taleb and R. Zagrouba, "Authentication scheme for IoT," in *2020 International Conference on Computing and Information Technology (ICCIIT-1441)*, IEEE, Sep. 2020, pp. 1–5. doi: 10.1109/ICCIIT-144147971.2020.9213714.
- [2] Y. Chen, X. Wang, Y. Yang, and H. Li, "Location-aware Wi-Fi authentication scheme using smart contract," *Sensors (Switzerland)*, vol. 20, no. 4, 2020, doi: 10.3390/s20041062.
- [3] M. Sugadev *et al.*, "Implementation of combined machine learning with the big data model in IoMT systems for the prediction of network resource consumption and improving the data delivery," *Computational Intelligence and Neuroscience*, vol. 2022, 2022, doi: 10.1155/2022/6510934.
- [4] R. Asif, K. Ghanem, and J. Irvine, "Proof-of-puf enabled blockchain: concurrent data and device security for internet-of-energy," *Sensors (Switzerland)*, vol. 21, no. 1, pp. 1–32, 2021, doi: 10.3390/s21010028.
- [5] A. Markose, S. Sharief, J. Ramprasath, and D. N. Krishnaraj, "Survey on application of IoT and its automation," *International Journal of Advanced Engineering Research and Science*, vol. 8, no. 6, pp. 245–251, 2021, doi: 10.22161/ijaers.86.29.
- [6] S. Sicari, A. Rizzardi, and A. Coen-Portisini, "5G in the internet of things era: qn overview on security and privacy challenges," *Computer Networks*, vol. 179, no. April, p. 107345, 2020, doi: 10.1016/j.comnet.2020.107345.
- [7] M. Tahir, M. Sardaraz, S. Muhammad, and M. S. Khan, "A lightweight authentication and authorization framework for blockchain-enabled IoT network in health-informatics," *Sustainability (Switzerland)*, vol. 12, no. 17, 2020, doi: 10.3390/SU12176960.
- [8] J. Li *et al.*, "A fast and scalable authentication scheme in IoT for smart living," *Future Generation Computer Systems*, vol. 117, pp. 125–137, Apr. 2021, doi: 10.1016/j.future.2020.11.006.
- [9] H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari, and H. Karimpour, "A survey on internet of things security: requirements, challenges, and solutions," *Internet of Things (Netherlands)*, vol. 14, p. 100129, 2021, doi: 10.1016/j.iot.2019.100129.
- [10] S. Pal, M. Hitchens, T. Rabehaja, and S. Mukhopadhyay, "Security requirements for the internet of things: a systematic approach," *Sensors (Switzerland)*, vol. 20, no. 20, pp. 1–34, 2020, doi: 10.3390/s20205897.
- [11] A. E. Omolara *et al.*, "The internet of things security: a survey encompassing unexplored areas and new insights," *Computers and Security*, vol. 112, p. 102494, 2022, doi: 10.1016/j.cose.2021.102494.
- [12] M. M. Ogonji, G. Okeyo, and J. M. Wafula, "A survey on privacy and security of internet of things," *Computer Science Review*, vol. 38. Elsevier Inc., p. 100312, 2020. doi: 10.1016/j.cosrev.2020.100312.
- [13] M. Elhoseny *et al.*, "Security and privacy issues in medical internet of things: overview, countermeasures, challenges and future directions," *Sustainability (Switzerland)*, vol. 13, no. 21, p. 11645, Oct. 2021, doi: 10.3390/su132111645.
- [14] M. El-Hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "A survey of internet of things (IoT) authentication schemes," *Sensors (Switzerland)*, vol. 19, no. 5, pp. 1–43, 2019, doi: 10.3390/s19051141.
- [15] S. Szymoniak and S. Kesar, "Key agreement and authentication protocols in the internet of things: a survey," *Applied Sciences (Switzerland)*, vol. 13, no. 1, p. 404, Dec. 2023, doi: 10.3390/app13010404.
- [16] A. Kumar, R. Saha, M. Conti, G. Kumar, W. J. Buchanan, and T. H. Kim, "A comprehensive survey of authentication methods in Internet-of-Things and its conjunctions," *Journal of Network and Computer Applications*, vol. 204, no. March. Elsevier Ltd, p. 103414, 2022. doi: 10.1016/j.jnca.2022.103414.
- [17] S. Kavianpour, B. Shanmugam, S. Azam, M. Zamani, G. Narayana Samy, and F. De Boer, "A systematic literature review of authentication in internet of things for heterogeneous devices," *Journal of Computer Networks and Communications*, vol. 2019, pp. 1–14, Aug. 2019, doi: 10.1155/2019/5747136.
- [18] D. Singh, B. Kumar, S. Singh, and S. Chand, "Evaluating authentication schemes for real-time data in wireless sensor network," *Wireless Personal Communications*, vol. 114, no. 1, pp. 629–655, 2020, doi: 10.1007/s11277-020-07385-0.
- [19] A. N. Bahache, N. Chikouche, and F. Mezrag, "Authentication schemes for healthcare applications using wireless medical sensor networks: a survey," *SN Computer Science*, vol. 3, no. 5, p. 382, Jul. 2022, doi: 10.1007/s42979-022-01300-z.
- [20] A. K. Gautam and R. Kumar, "A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks," *SN Applied Sciences*, vol. 3, no. 1, p. 50, Jan. 2021, doi: 10.1007/s42452-020-04089-9.
- [21] C. Wang, Y. Wang, Y. Chen, H. Liu, and J. Liu, "User authentication on mobile devices: approaches, threats and trends," *Computer Networks*, vol. 170, p. 107118, Apr. 2020, doi: 10.1016/j.comnet.2020.107118.
- [22] A. Srhir, T. Mazri, and M. Benbrahim, "Towards secure smart campus: security requirements, attacks and counter measures," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 32, no. 2, pp. 900–914, 2023, doi: 10.11591/ijeecs.v32.i2.pp900-914.
- [23] E. Dixit and V. Jindal, "IEESEP: an intelligent energy efficient stable election routing protocol in air pollution monitoring WSNs," *Neural Computing and Applications*, vol. 34, no. 13, pp. 10989–11013, 2022, doi: 10.1007/s00521-022-07027-5.
- [24] S. Dong, H. Su, Y. Xia, F. Zhu, X. Hu, and B. Wang, "A comprehensive survey on authentication and attack detection schemes that threaten it in vehicular Ad-Hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 12, pp. 13573–13602, 2023, doi: 10.1109/TITS.2023.3297527.
- [25] M. Mehic *et al.*, "Quantum cryptography in 5G networks: a comprehensive overview," *IEEE Communications Surveys and Tutorials*, pp. 1–1, 2023, doi: 10.1109/COMST.2023.3309051.
- [26] A. Haj-Hassan, Y. Imine, A. Gallais, and B. Quoitin, "Consensus-based mutual authentication scheme for Industrial IoT," *Ad Hoc Networks*, vol. 145, no. March, p. 103162, 2023, doi: 10.1016/j.adhoc.2023.103162.
- [27] E. S. Babu, A. K. Dadi, K. K. Singh, S. R. Nayak, A. K. Bhoi, and A. Singh, "A distributed identity-based authentication scheme for internet of things devices using permissioned blockchain system," *Expert Systems*, vol. 39, no. 10, Dec. 2022, doi: 10.1111/essy.12941.




- [28] A. Khurshid and S. Raza, "AutoCert: automated TOCTOU-secure digital certification for IoT with combined authentication and assurance," *Computers and Security*, vol. 124, p. 102952, 2023, doi: 10.1016/j.cose.2022.102952.
- [29] H. J. Mun and M. H. Lee, "Design for visitor authentication based on face recognition technology using CCTV," *IEEE Access*, vol. 10, pp. 124604–124618, 2022, doi: 10.1109/ACCESS.2022.3223374.
- [30] A. H. Ghafouri Mirsarai, A. Barati, and H. Barati, "A secure three-factor authentication scheme for IoT environments," *Journal of Parallel and Distributed Computing*, vol. 169, pp. 87–105, 2022, doi: 10.1016/j.jpdc.2022.06.011.
- [31] S. Kaur, G. Kaur, and M. Shabaz, "A secure two-factor authentication framework in cloud computing," *Security and Communication Networks*, vol. 2022, 2022, doi: 10.1155/2022/7540891.
- [32] Z. A. Zukarnain, A. Muneer, and M. K. Ab Aziz, "Authentication securing methods for mobile identity: issues, solutions and challenges," *Symmetry*, vol. 14, no. 4, MDPI, Apr. 2022. doi: 10.3390/sym14040821.
- [33] X. Jiang, R. Dou, Q. He, X. Zhang, and W. Dou, "EdgeAuth: an intelligent token-based collaborative authentication scheme," in *Software - Practice and Experience*, Apr. 2023. doi: 10.1002/spe.3206.
- [34] S. Yang, X. Zheng, G. Liu, and X. Wang, "IBA: a secure and efficient device-to-device interaction-based authentication scheme for Internet of Things," *Computer Communications*, vol. 200, no. September 2022, pp. 171–181, 2023, doi: 10.1016/j.comcom.2023.01.013.
- [35] G. Alqarawi, B. Alkhalifah, N. Alharbi, and S. El Khediri, "Internet-of-things security and vulnerabilities: case study," *Journal of Applied Security Research*, vol. 18, no. 3, pp. 559–575, Jul. 2023, doi: 10.1080/19361610.2022.2031841.
- [36] H. Taherdoost, "Security and internet of things: benefits, challenges, and future perspectives," *Electronics (Switzerland)*, vol. 12, no. 8, 2023. doi: 10.3390/electronics12081901.
- [37] C. Cao, Y. Tang, D. Huang, W. Gan, and C. Zhang, "IIBE: an improved identity-based encryption algorithm for WSN security," *Security and Communication Networks*, vol. 2021, pp. 1–8, Sep. 2021, doi: 10.1155/2021/8527068.
- [38] B. D. Deebak, F. H. Memon, S. A. Khowaja, K. Dev, W. Wang, and N. M. F. Qureshi, "In the digital age of 5G networks: seamless privacy-preserving authentication for cognitive-inspired internet of medical things," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 12, pp. 8916–8923, 2022, doi: 10.1109/TII.2022.3172139.
- [39] H. Huang, Q. Huang, F. Xiao, W. Wang, Q. Li, and T. Dai, "An improved broadcast authentication protocol for wireless sensor networks based on the self-reinitializable hash chains," *Security and Communication Networks*, vol. 2020, no. 1, pp. 1–17, Sep. 2020, doi: 10.1155/2020/8897282.
- [40] S. Karmakar, J. Sengupta, and S. Das Bit, "LEADER: low overhead rank attack detection for securing RPL based IoT," in *2021 International Conference on COMMunication Systems and NETWORKS, COMSNETS 2021*, 2021, pp. 429–437. doi: 10.1109/COMSNETS51098.2021.9352937.
- [41] H. Eltaief, "Flex-CC: a flexible connected chains scheme for multicast source authentication in dynamic SDN environment," *Computer Networks*, vol. 214, no. May, p. 109179, 2022, doi: 10.1016/j.comnet.2022.109179.
- [42] K. Haseeb, Z. Jan, F. A. Alzahrani, and G. Jeon, "A secure mobile wireless sensor networks based protocol for smart data gathering with cloud," *Computers & Electrical Engineering*, vol. 97, no. August 2020, p. 107584, Jan. 2022, doi: 10.1016/j.compeleceng.2021.107584.
- [43] C. Chunka, S. Banerjee, and R. S. Goswami, "An efficient user authentication and session key agreement in wireless sensor network using smart card," *Wireless Personal Communications*, vol. 117, no. 2, pp. 1361–1385, 2021, doi: 10.1007/s11277-020-07926-7.
- [44] Y. Xu, Y. Cao, Q. Liu, T. Li, and Q. Shan, "Simplified tree-based MPC for the cyber-physical system with jamming attacks," in *Proceedings - 2021 4th IEEE International Conference on Industrial Cyber-Physical Systems, ICPS 2021*, IEEE, 2021, pp. 891–897. doi: 10.1109/ICPS49255.2021.9468182.
- [45] S. M. U. Sankar, S. T. Revathi, and R. Thiagarajan, "Hybrid authentication using node trustworthy to detect vulnerable nodes," *Computer Systems Science and Engineering*, vol. 45, no. 1, pp. 625–640, 2023, doi: 10.32604/csse.2023.030444.
- [46] A. K. Maurya, A. K. Das, S. S. Jamal, and D. Giri, "Secure user authentication mechanism for IoT-enabled wireless sensor networks based on multiple bloom filters," *Journal of Systems Architecture*, vol. 120, no. September, p. 102296, 2021, doi: 10.1016/j.sysarc.2021.102296.
- [47] R. Qazi, K. N. Qureshi, F. Bashir, N. U. Islam, S. Iqbal, and A. Arshad, "Security protocol using elliptic curve cryptography algorithm for wireless sensor networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 1, pp. 547–566, Jan. 2021, doi: 10.1007/s12652-020-02020-z.
- [48] Ankit Gaur, "SPIN protocol in wireless sensor network," *International Journal of Engineering Research and*, vol. V9, no. 05, pp. 1305–1308, Jun. 2020, doi: 10.17577/ijertv9is050853.
- [49] T. Vandervelden, R. De Smet, K. Steenhaut, and A. Braeken, "Symmetric-key-based authentication among the nodes in a wireless sensor and actuator network," *Sensors*, vol. 22, no. 4, p. 1403, Feb. 2022, doi: 10.3390/s22041403.
- [50] Z. Zhang, W. Yang, F. Wu, and P. Li, "Privacy and integrity-preserving data aggregation scheme for wireless sensor networks digital twins," *Journal of Cloud Computing*, vol. 12, no. 1, 2023, doi: 10.1186/s13677-023-00522-7.

BIOGRAPHIES OF AUTHORS






Pendukeni Phalaagae    obtained an M.Sc. in Information Systems from the Botswana International University of Science and Technology in 2018 and acquired a B.Sc. in Data Communication and Computer Networks in 2011 from Multimedia University in Malaysia respectively. She is currently a Ph.D. student in Electrical, Computer and Telecommunications Department, Botswana International University of Science and Technology, Palapye, Botswana. She can be contacted at email: pendukeni.phalaagae@studentmail.biust.ac.bw.






Prof. Adamu Murtala Zungeru    (M'09–SM'18), Prof. Zungeru, holding Ph.D., M.Sc., and B.Eng. degrees, is a distinguished academic serving as the Professor and Head of the Department of Electrical, Computer, and Telecommunications Engineering at BIUST. His notable achievements include inventing a Termite-hill routing algorithm for Wireless Sensor Networks and a Method and System for Sorting Diamonds, with multiple patent applications. He has made substantial contributions with 5 academic books, over 70 international research articles, and editorial roles, including Associate Editor for IEEE Access Journal. His impact is reflected in an H-index of 15 and over 1,000 citations, particularly in renowned journals like IEEE Systems Journal and IEEE Internet of Things Journal. Additionally, he played significant roles in IEEE, including Chairmanship of the IEEE Botswana Sub-Section from 2019 to 2020. He can be contacted at email: zungerum@biust.ac.bw.



Dr. Boyce Sigweni    (M'18) received the B.Sc. degree in Computer Engineering from the University of KwaZulu-Natal, in 2007, the M.Sc. degree from North-West University, in 2011, and the Ph.D. degree in empirical software engineering from Brunel University London, U.K. He is currently a Senior Lecturer in computer engineering with the College of Engineering, Botswana International University of Science and Technology (BIUST). Prior to joining BIUST, he was a Computer Science Lecturer with North-West University. His research interests include powerline communication, next-generation networks, and empirical software engineering. He can be contacted at email: sigwenib@biust.ac.bw.



Prof. Selvaraj Rajalakshmi    an Associate Professor at BIUST's Department of Computer Science, holds a Ph.D. in Network Security. With over 12 years of experience, she actively engages in teaching, research, and strategic initiatives. Passionate about mentoring the next generation, she is currently working on a security system for honey pot architecture. As a member of research-promoting committees like IEEE and ACM. He has published over 60 articles, holds 4 international patents, and has supervised numerous M.Sc. and Ph.D. students. She can be contacted at email: selvarajr@biust.ac.bw.