STAP
Smart Technologies Academic Press

Journal of Cyber Security and Risk Auditing

https://www.jcsra.thestap.com/

A Novel Permissioned Blockchain Approach for Scalable and Privacy-Preserving IoT Authentication

Santosh Reddy Addula[1], Aitizaz Ali[2]

[1] *Department of Information Technology, University of the Cumberlands, Williamsburg, Kentucky, USA*
[2] *School of Technology, Asia Pacific University of Technology and Innovations, Kuala Lumpur, Malaysia*

ARTICLE INFO

Article History

Received: 17-03-2025
Revised: 10-06-2025
Accepted: 17-06-2025
Published: 20-06-2025

Vol.2025, No.4

DOI:
https://doi.org/10.63180/jcsra.thestap.2025.4.3

***Corresponding author.**
Email:
aitizaz.ali@apu.edu.my

Orcid:

https://orcid.org/0000-0002-4853-5093

ABSTRACT

Most existing research on decentralized IoT applications tends to address specific vulnerabilities, with relatively few techniques dedicated to managing privacy and trust issues. To mitigate these challenges, blockchain-based solutions are increasingly adopted to enhance the reliability and security of IoT networks. In particular, blockchain-based authentication frameworks offer a decentralized approach to storing and verifying device identities, enabling secure and trustless communication among devices and with external systems. However, current blockchain-based IoT systems often suffer from complexity and storage overhead. To address these limitations, we propose a novel solution tailored for large-scale IoT environments using a permissioned blockchain. Our approach incorporates optimized data storage and a lightweight authentication mechanism, offering improved scalability and reduced storage demands. Furthermore, we introduce, for the first time, the integration of homomorphic encryption to secure IoT data at the user end before uploading it to the cloud. The proposed framework is evaluated through comprehensive simulations and compared with existing benchmark models. This research contributes a trust-aware security model that significantly enhances both the privacy and security of IoT services.

Keywords: Internet of Things (IoT), Authentication, Blockchain, Security of IoT networks, Homomorphic Encryption Privacy.

How to cite the article
Addula, S. R., & Ali, A. (2025). A Novel Permissioned Blockchain Approach for Scalable and Privacy-Preserving IoT Authentication. Journal of Cyber Security and Risk Auditing, 2025(4), 222–237. https://doi.org/10.63180/jcsra.thestap.2025.4.3

1. Introduction

The rapid expansion of industrial Internet of Things (IoT) applications and networking services has led to a significant surge in the number of connected devices. These devices, equipped with dedicated sensor units, are capable of capturing real-time industrial data [1]. This shift in system interaction—driven by industrial advancements and technological innovation—facilitates seamless communication between physical and digital components. Traditionally, centralized architectures have been employed to manage and transmit industrial IoT data, including critical aspects such as identity management [2]. However, reliance on a centralized structure introduces a single point of failure, presenting significant system vulnerabilities [3]. Managing and maintaining the vast ecosystem of IoT devices remains a key challenge due to their scale and heterogeneity [4]. With adaptive self-configuration, networks can interact dynamically, supporting the commercialization of IoT applications over next-generation infrastructures like 6G. A core element in IoT ecosystems is the wireless sensor network (WSN), which captures and transmits physical data through various heterogeneous models [5].

Security is a paramount concern in IoT systems, especially as data generated by connected devices is stored in the cloud and transmitted over multiple networks [6]. In sensitive domains such as smart healthcare, cyber-attacks can result in severe operational and financial consequences. These include service disruptions, data breaches, power outages, and complete system compromise [7]. Monitoring complex smart grids to detect evolving threats is a major challenge for cybersecurity experts. Although machine learning has become integral to modern cybersecurity, managing the vast and diverse data generated within smart infrastructures requires distinct theoretical and practical approaches [8]. To analyze potential threats, threat modeling techniques are used to simulate various attack vectors, including spoofing, tampering, repudiation, information disclosure, denial of service (DoS), and elevation of privilege (EoP). These risks are systematically identified and addressed using the STRIDE threat model [9]. Additionally, the MITRE ATT&CK framework enables the mapping of real-world threat behaviors based on tactics, techniques, and procedures (TTPs) [10].

Blockchain technology has emerged as a promising solution to many of the IoT security challenges [11]. Blockchain offers a decentralized architecture underpinned by consensus mechanisms and smart contracts, which trigger specific actions based on predefined conditions [12, 13]. Blockchain implementations can be categorized into private, public, and hybrid models. Private blockchains restrict access within a single organization; public blockchains provide open access via public APIs and allow interaction with external networks such as gateways and cloud services. Hybrid or consortium blockchains combine elements of both, offering flexible access while maintaining operational security. In this study, a hybrid blockchain is utilized to interact with IoT systems for enhanced security and interoperability.

A key innovation in the proposed model is the integration of homomorphic encryption—introduced here for the first time. This encryption technique allows user data to be encrypted at the device level and securely outsourced to the cloud, enabling statistical and machine learning operations on encrypted data without compromising privacy. The IoT environment under study involves thousands of miniature sensors attached to patients' bodies, collecting real-time physiological data such as heart rate, blood pressure, temperature, and glucose levels. This generates vast datasets requiring robust training, testing, validation, and secure authentication. While existing IoT management systems provide basic functionalities, they often fall short in ensuring efficient and secure authentication. To address these limitations, the proposed model leverages a hybrid deep learning framework to process healthcare data and predict patient conditions autonomously, reducing the need for direct clinical intervention. This framework emphasizes lightweight authentication, privacy preservation, and comprehensive security. The key contributions of this research include: (1) the development of a novel trust-aware IoT framework that enhances privacy and security across connected IoT services. (2) The deployment of dedicated sensing units to capture industrial data across specialized network structures, reinforcing service orchestration. (3) A network architecture designed to support 6G-enabled IoT environments, incorporating diverse and trustworthy devices, and optimizing performance through biometric, video, and audio data integration.

2. Related Works

Blockchain technology has emerged as a promising tool to build trust and monitor node activity within Internet of Things (IoT) networks. However, integrating blockchain into IoT environments presents challenges, primarily due to high power consumption and the complexity of computation and task outsourcing [14]. Recent advancements have addressed these challenges through innovative blockchain-based IoT applications. For instance, certain blockchain implementations now allow for the deletion of older transactions and blocks without compromising network security.

The study [15] developed a blockchain-based IoT resource management prototype leveraging smart contracts to securely log all IoT transactions. Deploying smart contracts involves evaluating source code, compiled bytecode, and execution history, which forms the basis for simulating traffic analysis scenarios. Similarly, [16] explored blockchain and smart contract integration in cloud storage services, applying this to a pay-as-you-go car rental model that benefits from the technology's inherent traceability and tamper-proof characteristics. In another contribution, [17] proposed a blockchain-based publisher–subscriber model designed to ensure data integrity in real-time IoT applications by balancing computational workloads. To reduce the computational burden on resource-constrained devices, [18] proposed delegating Proof-of-Work (PoW) mining tasks to nearby edge servers in blockchain-enabled mobile IoT systems. Studies [19, 20] addressed the challenge of securing biometric data—particularly finger vein data—in healthcare IoT systems. Due to the immutable nature of biometric identifiers, such data requires robust protection mechanisms to prevent replay attacks and identity theft. Their research proposed a novel authentication framework combining RFID and finger vein biometrics with a triplex approach involving blockchain, Particle Swarm Optimization (PSO), and Advanced Encryption Standard (AES) encryption. The framework operates in three stages: random pattern generation using biometric fusion, secure authentication via CIA-compliant encryption and steganography, and empirical validation of the overall system. Additionally, the integration of Wireless Sensor Networks (WSNs) with 6G architectures enables testing across a wide spectrum of IoT deployment models. Many IoT systems now use IPv6-based protocols such as 6LoWPAN to support data collection through low-power personal area networks and wearable devices [21, 22]. Authentication and Key Agreement (AKA) protocols further help maintain user data confidentiality [23], especially in large-scale public cloud environments that demand rigorous data protection measures [14].

Some studies have proposed Physical Layer Security (PLS) as an alternative to conventional cryptographic approaches. PLS secures communication by degrading signal quality at the attacker's end, thereby enhancing confidentiality without relying on encryption keys [15]. Compared to key-dependent cryptographic techniques, PLS reduces the overhead of key management and simplifies encryption and decryption processes [20]. It also utilizes lightweight signal processing algorithms, making it particularly suitable for resource-constrained IoT environments. With the proliferation of IoT devices and data, batch processing is becoming essential for analyzing large datasets in cloud-based infrastructures [21]. Privacy regulations remain a critical concern, and studies such as that by [16] have examined frameworks for safeguarding user passwords within the constraints of privacy legislation. In contrast to real-time systems, where public and private keys are commonly used for cryptographic exchanges, cloud environments pose risks if a shared secret key is compromised, allowing unauthorized access to private data [17].

According to Statista, the number of connected IoT devices is projected to reach 50 billion by 2030, indicating a rapidly expanding market. In this context, privacy-preserving blockchain frameworks—such as the Trust-Aware Blockchain Seamless Authentication Protocol (TAB-SAPP)—offer promising solutions for securing user identities and enabling seamless authentication. Smart architectural designs also play a role in enhancing device connectivity across physical networks. Industrial automation standards like Zigbee, Z-Wave, and Bluetooth Low Energy (BLE) remain popular in this space. Blockchain's peer-to-peer architecture enables decentralized communication among IoT devices, where consensus algorithms and smart contracts govern data sharing and system behavior. In such blockchain-enabled IoT environments, data is encrypted and stored in chained blocks, and smart contracts act as logic controllers to verify device identity, manage access permissions, and enforce operational rules [7].

Different IoT applications, particularly in the medical domain, require varying levels of security depending on the nature of the data and resource constraints. Identifying the most suitable encryption technique for protecting sensitive medical information is therefore critical [12]. Electronic sensors continuously collect patient health data and transmit it to healthcare systems. To prevent unauthorized access and ensure seamless operation, trust and data privacy must be established from the point of data collection [13]. As a result, encrypting medical data at the sensor level is essential. However, traditional cryptographic algorithms are often unsuitable due to limitations in computational complexity, battery life, and transmission bandwidth inherent to IoT devices [47–50]. Ongoing research is focused on developing lightweight encryption algorithms optimized for medical IoT environments. One such study evaluates eight cryptographic algorithms in terms of speed and memory usage to identify the most effective and balanced option for securing healthcare data against evolving threats [14].

Furthermore, robust authentication mechanisms are necessary to protect healthcare services from malicious access. Both client and server sides must be authenticated to maintain data integrity and confidentiality [15]. On the server side, authentication ensures that patient records are only accessible by authorized personnel, while on the client side, authentication protects against impersonation of legitimate services [20]. This is especially important in emergency

scenarios—such as when an unconscious patient arrives at a hospital and cannot manually provide credentials. In such cases, secure biometric identification becomes a viable solution, using modalities like palm vein or iris recognition [26]. Biometric authentication has gained prominence due to its combination of high security, reliability, and usability [23]. Among these methods, finger vein (FV) recognition stands out as one of the most secure biometric approaches. Unlike traditional authentication systems that store simple biometric templates, FV systems rely on unique morphological features of blood vein patterns to identify individuals. These biological traits are extremely difficult to forge or replicate, making FV-based systems highly resistant to spoofing and impersonation attacks. To further secure FV biometrics, researchers have proposed both unimodal and multimodal biometric systems. These systems typically extract distinctive features—such as junction points and angles between veins—to generate a unique biokey used for data encryption. In this process, an observation matrix captures the extracted biometric features, which are then encrypted using randomly generated keys [10]. Some researchers have also implemented multimodal biometric systems that combine FV with other traits such as retinal scans and fingerprints to enhance accuracy and resilience. However, despite these advancements, certain challenges remain. Studies such as those by [16] have highlighted that the proposed systems still suffer from high communication and computational overhead, which can be limiting in real-time and resource-constrained environments like IoT-based healthcare systems.

2.1 Overview of Blockchain Structure

Blockchain is a decentralized and distributed ledger technology designed to securely record transactions across a network of interconnected nodes without the need for a central authority [14]. Each block in the blockchain contains a group of verified transactions, and once a block is appended to the chain, it becomes immutable—ensuring tamper-proof integrity [17]. This immutability and transparency make blockchain an ideal solution for applications requiring secure data management. As illustrated in Figure 1, the blockchain's data structure is typically organized as a sequential linked list of blocks. Each block consists of a header, which includes a cryptographic hash of the previous block, a timestamp, and a nonce, along with a body containing a batch of transactions. The transactions within each block are organized using a Merkle tree, a binary tree structure that allows efficient and secure verification of transaction integrity [19].

Blockchain systems rely on a distributed ledger model in which all nodes within the network maintain a synchronized copy of the ledger. This distributed nature ensures redundancy and resistance to tampering, as changes to the ledger require consensus from a majority of nodes in the network [20]. The cryptographic hash functions and consensus mechanisms such as Proof of Work (PoW) or Proof of Stake (PoS) are central to maintaining the security and consistency of the blockchain [18]. Furthermore, each transaction on the blockchain is digitally signed using cryptographic keys, ensuring authenticity and non-repudiation [19]. The decentralized storage model also enhances data availability and fault tolerance by distributing identical copies of the blockchain across multiple peer nodes. In summary, the architecture and data model of blockchain are specifically engineered to offer secure, decentralized, and transparent data management, making it highly suitable for applications such as finance, supply chain, healthcare, and the Internet of Things (IoT).

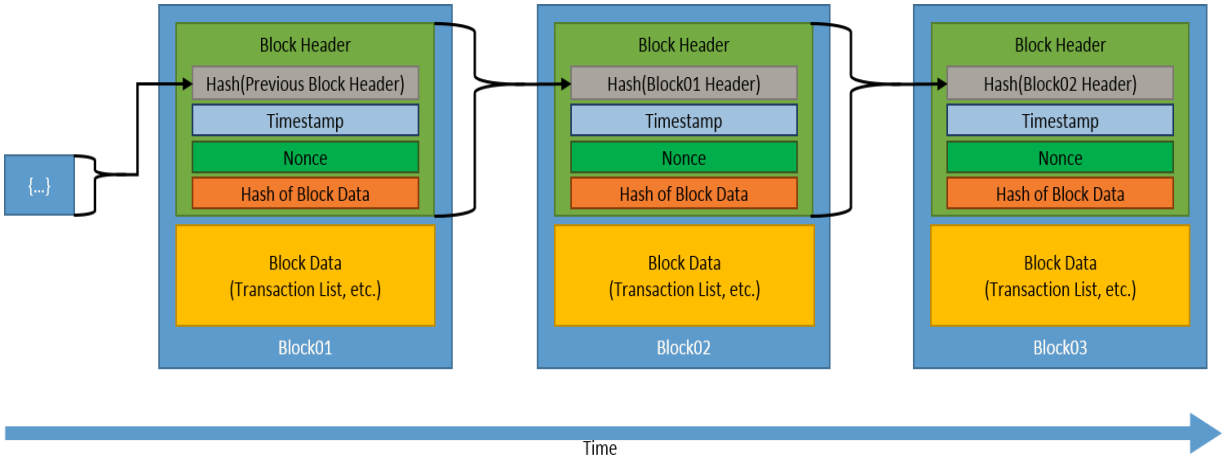

Figure 1. Structure of Blockchain.

2.2 IoT Data Flow

The Internet of Things (IoT) generates an extensive volume of data through a network of interconnected devices and sensors deployed across various domains. These devices—ranging from industrial equipment and household appliances to vehicles and smart home systems—continuously produce data such as sensor readings, geolocation (GPS) coordinates, and user interaction patterns. To ensure the integrity and trustworthiness of this data, IoT architectures increasingly incorporate blockchain technology. One of the key integration points is through the use of smart contracts—self-executing code that enforces the terms of an agreement embedded directly within the blockchain. These smart contracts automatically validate, log, and manage data transactions, thereby providing a secure, immutable, and transparent mechanism for handling IoT data.

As illustrated in Figure 2, a common method for authenticating IoT data involves programming smart contracts to verify the data's authenticity before it is committed to the blockchain ledger. This ensures that only verified and trustworthy data are stored, enhancing the reliability of the system [31]. By embedding authentication logic into smart contracts, data from IoT devices can be validated in real time, mitigating risks such as data falsification, unauthorized access, and replay attacks. In the context of this study, integrating smart contracts within IoT-blockchain ecosystems serves to strengthen the overall data governance framework. It offers a verifiable and automated method for authenticating IoT data, thereby contributing to the development of secure, decentralized, and tamper-resistant IoT applications.

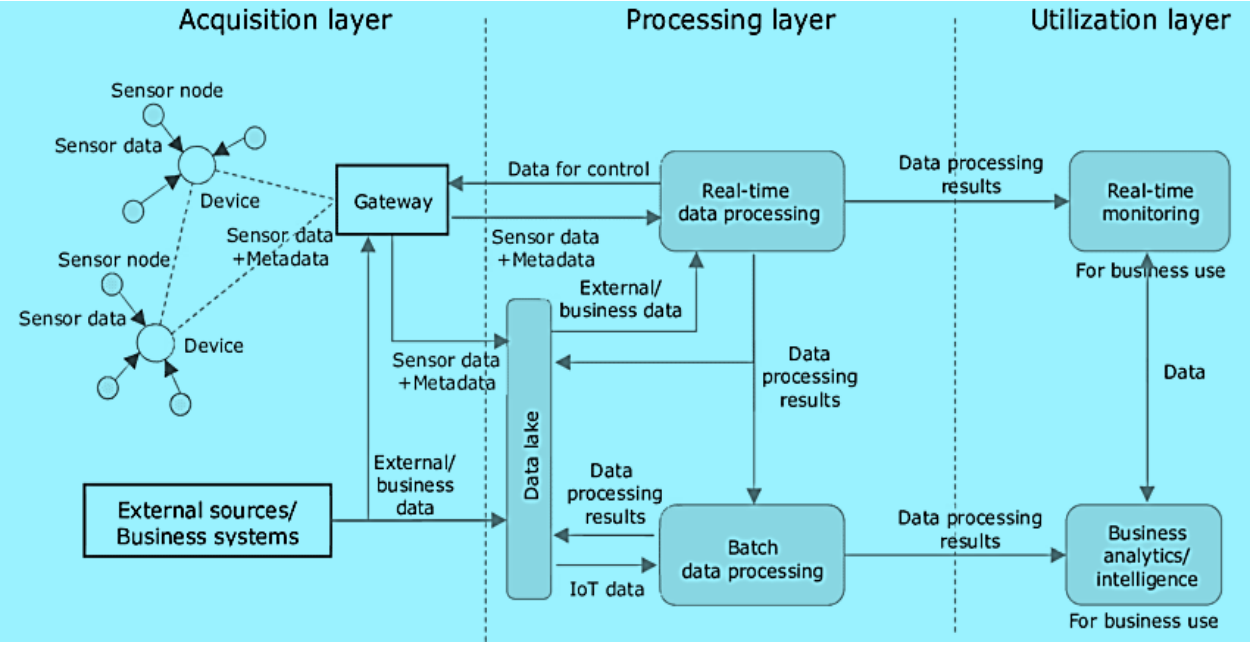

Figure 2. IoT Data Flow [1]

3. Methodology

The proposed methodology outlines a structured sequence of steps performed during the experimental phase to achieve the desired system output. Each step in the methodology is described in detail and visually supported by a schematic diagram illustrating the system workflow. In the first step, data are collected from IoT sensors and transmitted to a designated cluster head. In the second step, these data are processed through the blockchain, where they undergo verification and authentication from a large number of IoT edge devices. Following verification, the data are encrypted using homomorphic encryption and securely outsourced to the cloud. The integration of homomorphic encryption enables statistical and deep learning operations to be performed directly on the encrypted data without decryption, thereby preserving data privacy. The subsequent step involves feature extraction, where key attributes such as heart rate, age, sex, weight, and height are derived from the encrypted data. The framework then employs a Support Vector Machine (SVM) classifier to categorize

users and their corresponding data based on extracted features and system interaction. Finally, the output is verified and validated using a dedicated validation model to ensure accuracy and reliability.

3.1. Proposed Algorithm

To implement the proposed framework, a novel algorithm has been developed to manage core system functions. This algorithm is presented in Algorithm 1, which outlines the procedures for creating, updating, and revoking access to Personal Health Records (PHRs). Initially, the algorithm creates a new PHR upon receiving a user request. It then allows for the update of existing records, and if any access control policies are violated, it proceeds to revoke access. Algorithm 1 also defines the specific attributes assigned to both patients and clinicians to facilitate secure and role-based access control within the system.

Algorithm 1 presented for creating, updating, and revoking records in a blockchain network ensures secure and tamper-proof management of data throughout its lifecycle. It begins by authenticating the user's identity using a public-key-based digital signature to verify that only authorized entities can perform operations. For creating a new record, the algorithm first checks if the record already exists to avoid duplication. If the record is unique, it is written to the blockchain along with its data, a timestamp, and a cryptographic signature, ensuring immutability and traceability. When updating an existing record, the algorithm does not alter the original data. Instead, it creates a new block that references the previous block's hash, preserving the full history of changes. This approach provides transparency and enables auditability, which is particularly important in domains like healthcare or financial services. To revoke a record, the algorithm appends a new block with a "REVOKED" status, thereby maintaining the original data while indicating that it is no longer valid. This method supports data deactivation without deletion, preserving the integrity

and consistency of the blockchain ledger. The algorithm is lightweight and suitable for IoT environments where devices may have limited computational resources. Its design also facilitates integration with smart contracts to automate validation, enforce policies, and enhance security. Overall, this approach addresses key concerns in IoT security by providing a decentralized, transparent, and efficient framework for managing digital records.

Algorithm 1. Create, Update and Revoke Records in blockchain

```
1. Authenticate User (UserKey)
  a. IF User Key is not authorized THEN
       RETURN "Access Denied"
  b. ELSE
       CONTINUE
2. SWITCH(Action)
    CASE 'CREATE':
     a. IF Record ID already exists in Blockchain THEN
          RETURN "Error: Record already exists"
     b. ELSE
          Create Record Block with:
            - RecordID
            - Data = New Data
            - Timestamp = Current Time()
            - Action = "CREATE"
            - Status = "ACTIVE"
            - Signature = Sign(Data, User Key)
          Append Record Block to Blockchain
          RETURN "Record successfully created"
  CASE 'UPDATE':
     a. IF RecordID not found OR Status ≠ "ACTIVE" THEN
          RETURN "Error: Record not found or inactive"
     b. ELSE
```

```
        Create Update Block with:
          - RecordID
          - Updated Data = New Data
          - Timestamp = Current Time()
          - Action = "UPDATE"
          - Previous Hash = Get Hash Of Las tRecord (RecordID)
          - Signature = Sign(New Data, User Key)
        Append Update Block to Blockchain
        RETURN "Record successfully updated"

    CASE 'REVOKE':
      a. IF RecordID not found OR Status ≠ "ACTIVE" THEN
          RETURN "Error: Record not found or already revoked"
      b. ELSE
          Create Revoke Block with:
            - RecordID
            - Timestamp = Current Time()
            - Action = "REVOKE"
            - Signature = Sign(RecordID + Action, User Key)
          Append Revoke Block to Blockchain
          Set Status of RecordID = "REVOKED"
          RETURN "Record successfully revoked"
```

Algorithm 2 is responsible for validating user attributes by assigning a master key, a signature count, and initializing the bilinear pair groups—typically denoted as G1and G2. Within this framework, the user randomly selects a value from these groups to initiate secure communication and authentication. This algorithm plays a crucial role in evaluating the system's response to user requests by verifying the correctness and integrity of the assigned attributes. It checks whether the parameters and credentials presented by the user match those that have been pre-established within the system. The evaluation ensures that only legitimate users with valid attributes can access or interact with the system. Furthermore, Algorithm 2 outlines the application of homomorphic encryption in the authentication and processing stages of the model. This cryptographic method enables computations to be performed directly on encrypted data, eliminating the need to decrypt it first. This significantly enhances data privacy and security, especially when handling sensitive information like health records or personal identifiers in IoT environments. The integration of homomorphic encryption ensures that the system can perform essential operations—such as authentication, classification, or statistical analysis—without exposing raw data, thereby maintaining end-to-end confidentiality and strengthening the trust model in distributed IoT architectures.

Algorithm 2. Validating user attributes by assigning a master key

1. **Initialization:**
1.1. Select bilinear groups G1, G2 and a bilinear map e: $G1 \times G1 \rightarrow G2$
1.2. Generate master key MK and public parameters PP
1.3. Set up hash functions H1,H2 for identity and attribute encoding

2. **User Key Generation:**
2.1. User selects a random secret $r \in G1$
2.2. Compute public key $PK = r \cdot G$ where G is a generator of *G1*
2.3. Sign attributes using digital signature scheme
2.4. Send {*PK, Attributes, Signature*}to the verifier

3. **Attribute Verification:**
3.1. Verifier checks digital signature with public parameters *PP*
3.2. If signature is valid, proceed; else Reject Request

3.3. Compare received attributes with access policy
3.4. If attributes satisfy policy, proceed; else Reject Request

4. **Homomorphic Encryption Setup:**
4.1. For each attribute $a_i \in Attributesa\_$
4.1.1. Encrypt using homomorphic encryption scheme:
$EA_i = HE\_Encrypt\ (a_i, PK)$
4.2. Store EA={EA1,EA2,...,EAn} on blockchain

5. **Return:**
Status = Authenticated
Return Encrypted Attributes *EA*

Algorithm 3 outlines the procedure for selecting a cluster head within the IoT network. The selection is determined based on the available battery power of the sensor nodes. Among the nodes, the one with the highest remaining power is designated as the cluster head. Once selected, the cluster head is responsible for receiving IoT data from the other sensor nodes in the network, thereby facilitating efficient communication and energy management.

Algorithm 3. Selection of Cluster Head

1. **Initialize:**
   Set CH ← null
   Set maxBattery ← 0
2. **For each node** $n_i \in N$ **do**
   a. Measure battery level $B(n_i)$
   b. If $B(n_i) > maxBattery$ then
      i. $maxBattery \leftarrow B(n_i)$
      ii. $CH \leftarrow n_i$
3. **End For**
4. Return CH as the selected Cluster Head.

Algorithm 4 outlines the step-by-step procedure for encrypting Electronic Medical Records (EMR) using Homomorphic Encryption (HE). Homomorphic encryption enables mathematical and statistical computations to be performed directly on encrypted data, eliminating the need for decryption beforehand. This capability ensures that sensitive health information remains secure and private throughout the data processing lifecycle. In the proposed model, HE allows users to encrypt their data locally and securely outsource it to the cloud for processing. Among the three main types of homomorphic encryption—fully homomorphic encryption (FHE), partially homomorphic encryption (PHE), and hybrid HE—this study employs FHE. This choice aligns with the system's requirements, particularly the need to support complex computations across a large number of Internet of Medical Things (IoMT) devices, while maintaining strong privacy guarantees.

Algorithm 4. EMR Encryption Using Fully Homomorphic Encryption (FHE)

1. **Initialize FHE Scheme**
Generate a key pair:
$(pk,sk) \leftarrow HE.KeyGen()$
2. **Data Collection**
Acquire raw EMR data from IoMT devices (e.g., heart rate, temperature, glucose levels).
$D=\{d1,d2,...,dn\}$
3. **Encrypt EMR Data**
For each data element $di \in D$:
E(di)=*HE.Encrypt (pk,di) E(d_i)*
4. **Form Encrypted Dataset**

Combine encrypted elements:
$E(D)=\{E(d1),E(d2),...,E(dn)\}$
5. **Outsource to Cloud**
Transmit $E(D)$ securely to the cloud for storage or processing.
6. **Perform Encrypted Computations**
Allow statistical or machine learning operations over $E(D)$ using:
$HE.Eval(f,E(D))$, where f is a supported function (e.g., sum, average).
7. **Return:**
Encrypted dataset $E(D)$

Algorithm 4 outlines a systematic approach to encrypting Electronic Medical Records (EMR) using Fully Homomorphic Encryption (FHE), ensuring end-to-end data confidentiality and privacy preservation within IoMT (Internet of Medical Things) environments. The algorithm begins by initializing the FHE scheme and generating a secure key pair. This foundational step is crucial for enabling secure encryption and subsequent operations on the data. Once the IoMT devices collect patient-specific medical data (such as vital signs and biometric metrics), each data point is encrypted individually using the public key. This encryption step ensures that sensitive health data are transformed into a cipher text form that is unintelligible to unauthorized users, including third-party cloud providers. A critical advantage of using FHE, as demonstrated in this algorithm, is the ability to perform meaningful computations—such as statistical analysis or machine learning inference—directly on encrypted data without requiring decryption. This feature eliminates the security risk typically associated with decrypting data before processing, thereby preserving privacy throughout the data lifecycle.

After encryption, the data are outsourced to a cloud server, where they can be stored securely or used for encrypted computations. This model is particularly well-suited for healthcare systems that need to process large volumes of data while complying with strict regulatory requirements such as HIPAA or GDPR. The choice of FHE, rather than partially or hybrid homomorphic encryption, is deliberate in this context. FHE provides maximum flexibility for supporting diverse and complex operations over encrypted data—an essential requirement for healthcare applications involving predictive analytics or AI-driven diagnostics. In summary, Algorithm 4 plays a vital role in enabling secure, scalable, and privacy-preserving data handling in IoMT networks. It addresses key concerns related to data confidentiality, unauthorized access, and compliance, making it an essential component in the design of modern, secure healthcare information systems.

3.2. System Model

This section introduces a secure and efficient industrial automation authentication system designed to ensure trustworthiness and simplicity. The system leverages a multi-signature-compatible smart contract to verify private keys, ensuring that unauthorized access is prevented. Within the context of industrial automation, the model adopts a pay-as-you-go intelligent framework to evaluate and manage the computational processes of IoT devices effectively. As illustrated in Figure 2, the Internet of Things (IoT) ecosystem encompasses a vast network of components—including thousands to millions of sensors, edge devices, computing units, Wi-Fi modules, and RFID tags—all generating large volumes of data. The scale and heterogeneity of this data make it particularly susceptible to security breaches and data mismanagement. The use of multi-signature-compatible smart contracts allows for comprehensive assessment of each transaction's integrity, covering everything from quality assurance and operational procedures to automated decision-making. These contracts enable the system to analyze traffic patterns and make autonomous decisions that improve system intelligence and responsiveness. Smart contracts are further utilized to assess the core functional behavior of each IoT device, optimizing the performance and efficiency of the entire network. The model ensures scalability, resilience, and reliability in processing industrial IoT operations. Table 1 presents the application of the TAB-SAPP framework, which demonstrates how researchers formalize trust-aware authentication protocols within this context.

Table 1. Simulation setup

Parameters	Details
Dataset size	150 number of blocks + PHR
Hardware Software Parameters	GPU-enabled system Ethereum, hyperledger fabric

Performance Metric	Block height, number of blocks, No. transactions, No. PHR, delay, signature creation
Number of simulations Number of rounds or transactions	Efficiency (average percentage of Gas, no. packets, no. dead nodes, no. alive nodes), security (the execution time of policies) and cost (execution time of blocks), Number of tests performed on single dataset: 6000

Consumers frequently rely on Internet of Things (IoT) devices to execute transactions remotely through decentralized IoT networks. These transactions, especially in industrial contexts, require secure authentication and proper registration mechanisms. In this setting, Web3API-based interactions depend on a valid contract state to proceed. A billfold contract serves as a secure gateway, enabling clients to access industrial assets and register large-scale IoT devices on the network. Complementing this, a control contract permits public validation of the device's status, ensuring transparency and reliability in its operations [35]. The proposed Trust-Aware Blockchain-based Smart Authentication and Privacy Preservation (TAB-SAPP) framework utilizes smart contracts to handle critical functions such as whitelisting, device registration, payment processing, key generation, and secure device operations. For secure authentication, consumer signatures are created using the 256-bit Keccak hashing algorithm in combination with Elliptic Curve Digital Signature Algorithm (ECDSA). This mechanism ties the user's identity, the IoT device, and the control contract through a unique private key, forming a secure interaction environment.

In the initial phase, an external owner account is responsible for establishing a whitelist, which defines access rights and permitted interactions with the system. The control contract then specifies a transaction fee, which users must pay to gain access to IoT services. This fee also applies to any blockchain participant who wishes to validate the transaction. Once the whitelist is created, the client and the IoT device are linked to the external owner account, ensuring that contractual operations consider the user's needs and access privileges [12].

Following successful registration, the IoT device processes the necessary fee payments to finalize its enrollment in the system. The TAB-SAPP framework ensures that all steps—from device whitelisting to payment and key computation—are governed securely through smart contracts using encrypted signatures. These operations leverage ECDSA and Keccak hash functions to maintain the confidentiality and integrity of all transmitted data. Furthermore, the contract organization is tasked with maintaining and updating the whitelist as well as the associated fee structures. During a data transaction, multi-signature verification is employed to ensure the validity and authenticity of the exchange. This method imposes a shared verification cost among all parties involved, enhancing both trust and accountability [16].

Finally, the linkage between consumers, IoT devices, and the external owner account is essential for completing secure device registration and ensuring that only authorized devices are allowed to interact with the blockchain. After registration and payment, the IoT device can operate securely within the network, while the contract infrastructure ensures consistent compliance and secure communication across the ecosystem [17].

3.3 Elliptic Curve for Alternate Key

The proposed approach leverages Elliptic Curve Cryptography (ECC) for secure key distribution and digital signature exchange, offering enhanced security with reduced computational overhead—making it ideal for IoT environments. ECC enables the generation of compact keys while maintaining a high level of cryptographic strength. This is particularly important for resource-constrained IoT devices that need lightweight yet robust security mechanisms.

Additionally, the model integrates ring signatures to ensure user anonymity and trust during authentication processes. Ring signatures allow any member of a group to sign a message on behalf of the group without revealing which member actually signed it, thereby enhancing privacy and unlink ability among IoT users [18].

The foundation of ECC is the elliptic curve equation defined as follows:

$$y^2 \bmod q = (x^3+ax+b) \bmod q \qquad (1)$$

Where: x and y are the coordinates of a point on the elliptic curve, a and b are curve parameters that define the shape of the curve and q is a large prime number that serves as the modulus, defining a finite field over which the curve is defined. This equation forms the basis for generating the elliptic curve group $E(q)$, from which public and private keys are derived. The key distribution, digital signing, and verification operations are carried out using points on this curve, ensuring cryptographic integrity and confidentiality in the IoT system. The integration of ECC with ring signatures in the proposed framework provides a powerful and efficient mechanism for securing IoT communications, enabling trust-aware authentication while minimizing computational burden.

Then $P(x,y)$ is a valid point on the elliptic curve $Eq(a,b)$. Each point on the elliptic curve has an additive inverse that is symmetric about the x-axis. That is, if $P(x,y)$ is a point on the curve, then the point $Q(x,-y \bmod q)$ is its negative, denoted as -P and satisfies $P+(-P)=O$, where O is the point at infinity, or the identity element of the elliptic curve group.

Now, consider two distinct points $P(x_1, y_1)$ and $Q(x_2, y_2)$ on the curve $Eq(a,b)$ and let $P \neq Q$. The line l that passes through these two points intersects the elliptic curve at a third point $R_0=(x_3,y)$. Due to the symmetric property of elliptic curves, the reflection of R_0 about the x-axis is the point $R=(x_3, y_3)$, where $y_3 = -y \bmod q$. This point R is defined as:

$$R = P + Q \qquad (2)$$

This point addition rule forms the basis of scalar multiplication on elliptic curves, which is the fundamental operation used in elliptic curve cryptography for key generation, digital signatures, and encryption. If the same point is added to itself repeatedly, such as $p+p+\cdots+p$ (six times), the result is denoted as $6P=Q$, a form of scalar multiplication. These properties make elliptic curves highly suitable for cryptographic protocols, offering strong security with smaller key sizes and efficient computations, which are particularly beneficial in IoT environments.

4. Experimental Setup

To implement and evaluate the proposed system, a blockchain environment was established using the Hyperledger Fabric framework, which facilitated secure communication and transaction management among IoT nodes. The experimental setup focused on simulating a real-world industrial IoT scenario to assess the system's performance and security features. Key parameters recorded during the experiments included the number of IoT nodes, the number of operational rounds, the time taken for block creation and block digest computation, encryption time using homomorphic encryption, and access control enforcement time. The system used for simulation was equipped with a Core i7 processor, GPU acceleration, and ran on a Linux operating system to ensure high computational efficiency.

In terms of security validation, the proposed model was evaluated using AVISPA (Automated Validation of Internet Security Protocols and Applications) and METRE (Model-based Evaluation of Threats to Resources and Entities). AVISPA was employed to test the system's ability to withstand collusion and phishing attacks, while METRE was used to verify the access control and authentication mechanisms under dynamic threat conditions. These formal verification tools confirmed that the proposed model is resistant to common IoT security threats and offers reliable protection while maintaining performance efficiency in a decentralized network environment.

5. Analysis and Findings

Based on the findings illustrated in Figure 3, the proposed method demonstrates a notable improvement in the authentication process by integrating blockchain technology with mobility speed. This integration leverages the immutable and decentralized attributes of blockchain to enhance the reliability and security of authentication, while the inclusion of mobility speed ensures real-time responsiveness and adaptability in dynamic environments. As a result, the system provides a more robust and efficient authentication mechanism suited for modern, mobile-driven IoT ecosystems. The insights derived from these findings are especially relevant for organizations aiming to strengthen their authentication infrastructure in the context of ongoing digital transformation. By optimizing authentication through secure, decentralized processes and real-time data validation, the proposed system aligns well with the demands of increasingly mobile and connected networks. Furthermore, the comparative analysis, which evaluates performance based on the number of nodes and encryption time, underscores the efficiency of the proposed framework in comparison to existing benchmark models. As shown in Figure 3, the proposed approach consistently outperforms traditional models, affirming its capability to offer lower encryption

times while scaling effectively with a higher number of nodes. This makes it a viable and future-ready solution for industries seeking enhanced cybersecurity measures in IoT-based environments.

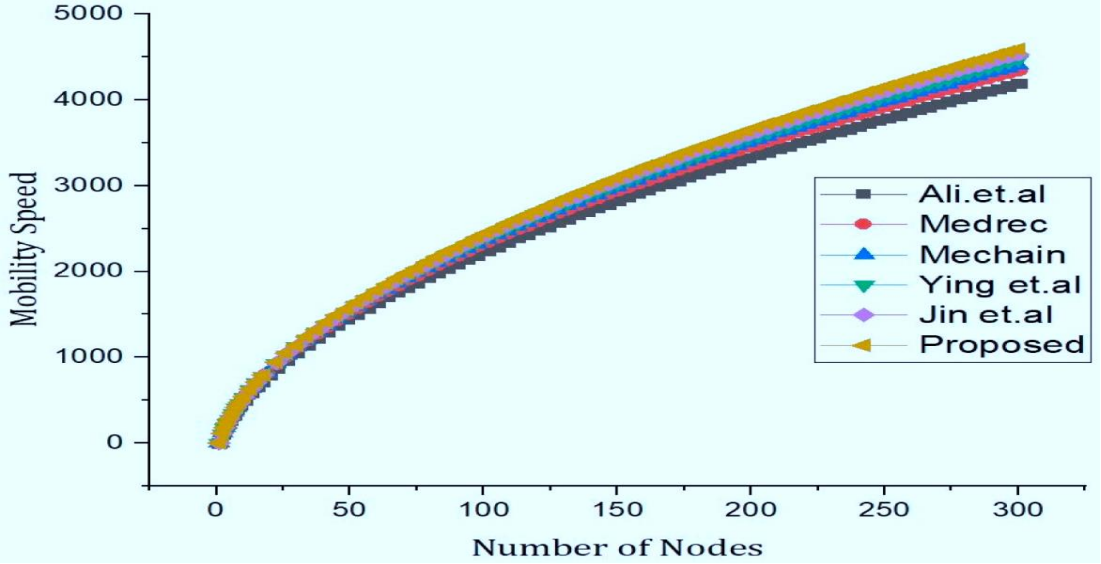

Figure 3. The comparative analysis of the proposed framework against benchmark models, based on speed and number of nodes

Figure 4 presents the simulation results highlighting the latency observed across each node within the system. The analysis clearly demonstrates that the proposed framework consistently maintains lower latency levels when compared to the benchmark models. This reduced latency is a key indicator of the framework's ability to process transactions and authenticate data more efficiently, even under increased network load. The low-latency performance can be attributed to the integration of blockchain technology with optimized encryption and authentication mechanisms, which minimize delays in data verification and access control. As a result, the proposed model not only enhances system responsiveness but also supports real-time decision-making—an essential feature for IoT applications with time-sensitive requirements. In conclusion, the results confirm that the proposed framework offers both efficiency and robustness, making it well-suited for scalable and performance-critical IoT environments.

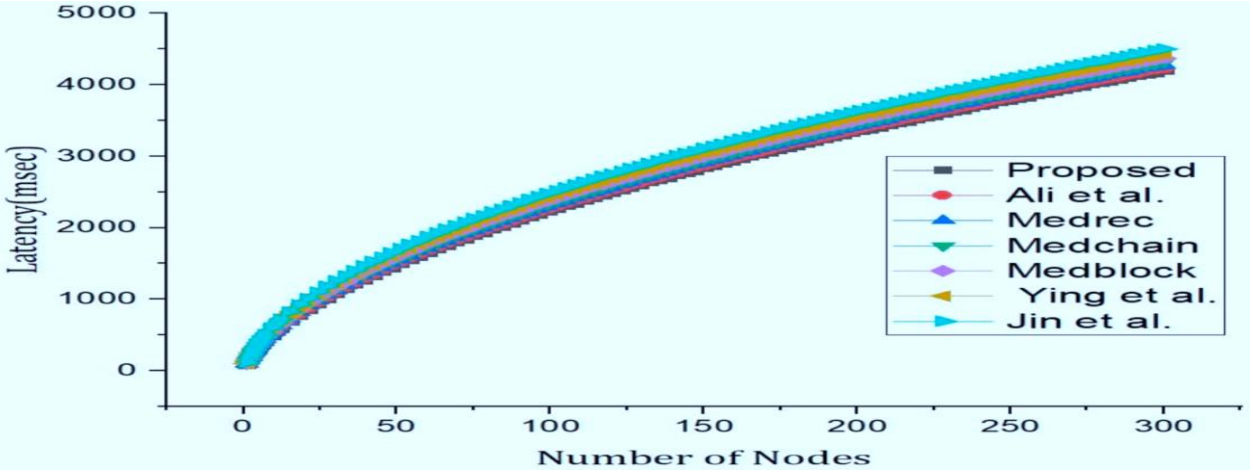

Figure 4. The comparative analysis between the proposed framework and benchmark models, based on latency and the number of nodes.

Figure 5 presents the comparative analysis based on the number of nodes versus encryption time demonstrates that the proposed framework offers superior scalability and efficiency compared to benchmark models. As the number of IoT nodes increases, the encryption time in traditional models rises significantly due to higher computational overhead and less optimized encryption schemes. In contrast, the proposed framework maintains relatively lower and more consistent encryption times across varying node densities. This performance advantage is attributed to the implementation of fully homomorphic encryption, which is optimized within the framework to support parallel processing and reduced complexity. Additionally, the use of cluster-head selection and lightweight cryptographic algorithms helps to distribute the workload efficiently, minimizing bottlenecks in encryption operations. This efficient handling of encryption tasks, regardless of node growth, ensures that the proposed model remains practical and responsive even in large-scale IoT networks. Therefore, the results confirm the suitability of the proposed system for real-time, secure communication in environments with high node density.

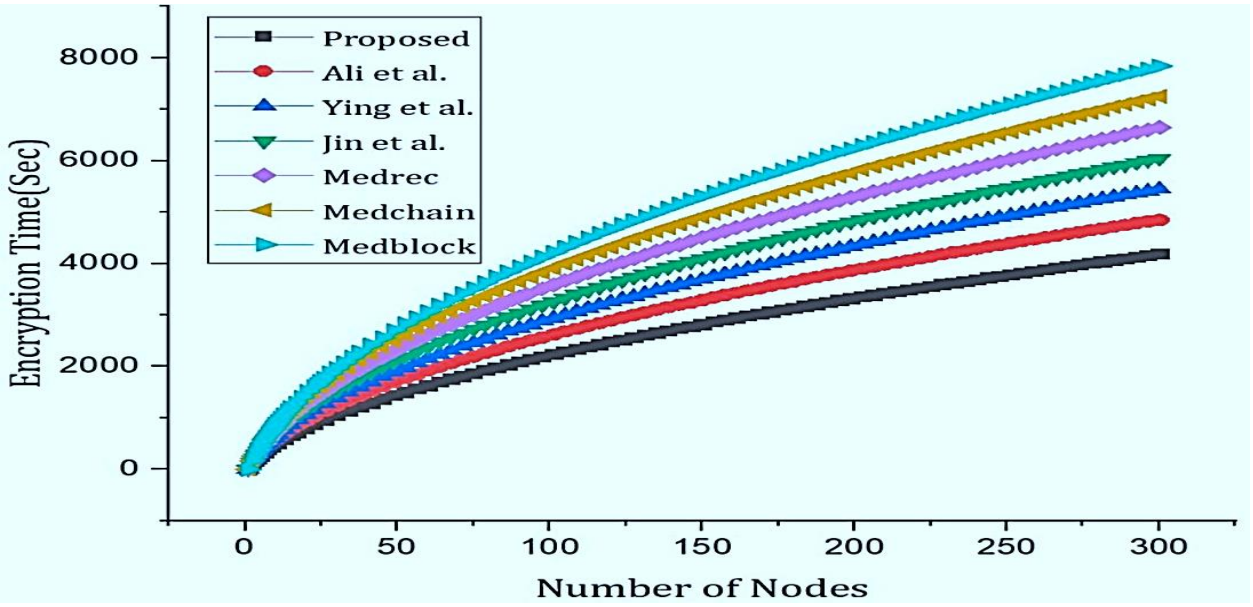

Figure 5. The comparative analysis based on the number of nodes versus encryption time.

To evaluate the attack resistance of the proposed framework, a comparative analysis was conducted with benchmark models, as shown in Table 2. This evaluation considers the framework's ability to withstand various cybersecurity threats, including collusion attacks, phishing attacks, replay attacks, and man-in-the-middle attacks. The analysis demonstrates that the proposed framework outperforms benchmark models in multiple aspects. This enhanced resilience is primarily due to the integration of blockchain-based authentication, fully homomorphic encryption, and a trust-aware security mechanism. Blockchain provides an immutable, decentralized ledger that ensures tamper-proof identity verification and traceability, significantly reducing the risk of unauthorized access and identity spoofing. Furthermore, the use of multi-signature smart contracts and elliptic curve cryptography (ECC) strengthens the authentication layer, making it more resistant to key compromise and forgery. The application of homomorphic encryption adds another security layer by enabling secure computations on encrypted data, minimizing exposure during data processing. As a result, the proposed framework achieves a higher level of attack resistance across diverse IoT scenarios, making it particularly well-suited for sensitive domains such as healthcare, smart cities, and industrial automation where security is paramount.

Table 2. Comparative Analysis of Attack Resistance

Attack Type	Merdec	Mechain	Ali et al.,	Proposed Framework
Collusion Attack	✗	✓	✗	✓
Phishing Attack	✗	✗	✓	✓
Replay Attack	✗	✗	✗	✓

Man-in-the-Middle Attack	✓	✗	✗	✓
Key Forgery	✗	✗	✗	✓
Unauthorized Access	✓	✗	✗	✓

6. Conclusions and Future Work

This study presented a privacy-preserving authentication framework tailored for industrial IoT applications. The proposed system integrates hash evaluation and MAC verification to minimize computational and communication overhead. It supports large-scale IoT deployments and ensures user identity protection through service deniability, even over unsecured networks. By leveraging authenticated data blocks and efficient data transmission, the framework demonstrates superior performance in terms of computation speed, connectivity, and mobility, thereby enhancing the overall security and efficiency of data processing and communication.

The primary objective of this research was to minimize end-to-end latency while maintaining a robust authentication mechanism. Comparative analysis with existing benchmark models confirms that the proposed solution significantly improves authentication processes by integrating blockchain technology with dynamic mobility parameters. The immutability and decentralization of blockchain, combined with real-time responsiveness, result in a secure, reliable, and efficient authentication framework. These contributions provide meaningful insights for organizations aiming to optimize their authentication infrastructure in the context of rapid digital transformation.

However, a notable limitation of this work is its reliance on a single permissions-based blockchain mechanism. Although this approach offers lightweight authentication and optimized data storage via smart contracts, broader applicability may require increased flexibility and robustness. As part of future work, the framework can be extended by incorporating consensus algorithms to improve trust and reliability. In addition, we plan to integrate advanced deep learning techniques with blockchain technology to enable trust-based user classification. Enhancements will also include the incorporation of software-defined networking (SDN) and 5G technologies to improve real-time responsiveness and scalability. Furthermore, the proposed model may be extended to emergency rescue systems, enabling secure and timely communication in critical scenarios using blockchain for reliable data integrity and delivery.

Corresponding author

Dr. Aitizaz Ali
aitizaz.ali@apu.edu.my

Acknowledgements
NA.

Funding
No funding.

Contributions
S.R.A; A.A; Conceptualization, S.R.A; A.A; Investigation, S.R.A; A.A;Writing (Original Draft), S.R.A; A.A;Writing (Review and Editing) Supervision, S.R.A; A.A; Project Administration.

Ethics declarations
This article does not contain any studies with human participants or animals performed by any of the authors.

Consent for publication
Not applicable.

Competing interests
The author declares no competing interests.

References

[1] Kim, S., Del Castillo, R. P., Caballero, I., Lee, J., Lee, C., Lee, D., ... & Mate, A. (2019). Extending data quality management for smart connected product operations. *IEEE Access*, *7*, 144663-144678.
[2] Sameera, K. M., Nicolazzo, S., Arazzi, M., Nocera, A., KA, R. R., Vinod, P., & Conti, M. (2024). Privacy-preserving in Blockchain-based Federated Learning systems. *Computer Communications*.
[3] Padma, A., & Ramaiah, M. (2024). Blockchain based an efficient and secure privacy preserved framework for smart cities. *IEEE Access*, *12*, 21985-22002.
[4] Liu, W. J., Chiu, W. Y., & Hua, W. (2024). Blockchain-enabled renewable energy certificate trading: A secure and privacy-preserving approach. *Energy*, *290*, 130110.
[5] Kasyap, H., & Tripathy, S. (2024). Privacy-preserving and byzantine-robust federated learning framework using permissioned blockchain. *Expert Systems with Applications*, *238*, 122210.
[6] Wu, X., Liu, Y., Tian, J., & Li, Y. (2024). Privacy-preserving trust management method based on blockchain for cross-domain industrial IoT. *Knowledge-Based Systems*, *283*, 111166.
[7] Reddi, S., Rao, P. M., Saraswathi, P., Jangirala, S., Das, A. K., Jamal, S. S., & Park, Y. (2024). Privacy-preserving electronic medical record sharing for IoT-enabled healthcare system using fully homomorphic encryption, IOTA, and masked authenticated messaging. *IEEE Transactions on Industrial Informatics*.
[8] Mahato, G. K., Banerjee, A., Chakraborty, S. K., & Gao, X. Z. (2024). Privacy preserving verifiable federated learning scheme using blockchain and homomorphic encryption. *Applied Soft Computing*, *167*, 112405.
[9] Bounceur, A., Berkani, A. S., Moumen, H., & Benharzallah, S. (2025). The Transparency Challenge in Blockchain-Enabled Sustainable Development Goals Applications: Exploring Privacy-Preserving Techniques and Emerging Platforms. *IEEE Access*.
[10] Dib, O. (2025). A Decentralized Privacy-Preserving Framework for Diabetic Retinopathy Detection Using Federated Learning and Blockchain. *Results in Engineering*, 105456.
[11] Tawfik, A. M., Al-Ahwal, A., Eldien, A. S., & Zayed, H. H. (2025). ACHealthChain blockchain framework for access control and privacy preservation in healthcare. *Scientific Reports*, *15*(1), 1-25.
[12] Sutradhar, S., Karforma, S., Bose, R., Roy, S., Djebali, S., & Bhattacharyya, D. (2024). Enhancing identity and access management using hyperledger fabric and oauth 2.0: A block-chain-based approach for security and scalability for healthcare industry. *Internet of Things and Cyber-Physical Systems*, *4*, 49-67.
[13] Rai, H. M., Shukla, K. K., Tightiz, L., & Padmanaban, S. (2024). Enhancing data security and privacy in energy applications: Integrating IoT and blockchain technologies. *Heliyon*, *10*(19).
[14] Kumari, D., Parmar, A. S., Goyal, H. S., Mishra, K., & Panda, S. (2024). HealthRec-Chain: Patient-centric blockchain enabled IPFS for privacy preserving scalable health data. *Computer Networks*, *241*, 110223.
[15] Ren, Z., Yan, E., Chen, T., & Yu, Y. (2024). Blockchain-based CP-ABE data sharing and privacy-preserving scheme using distributed KMS and zero-knowledge proof. *Journal of King Saud University-Computer and Information Sciences*, *36*(3), 101969.
[16] Kashif, M., & Kalkan, K. (2024). EPIoT: Enhanced privacy preservation based blockchain mechanism for internet-of-things. *Computer Networks*, *238*, 110107.
[17] Salim, M. M., Yang, L. T., & Park, J. H. (2024). Privacy-preserving and scalable federated blockchain scheme for healthcare 4.0. *Computer Networks*, *247*, 110472.
[18] Guo, X., Lu, X., Jiang, Y., Fang, J., & Zhang, D. (2024). DBCPCA: Double-layer blockchain-assisted conditional privacy-preserving cross-domain authentication for VANETs. *Ad Hoc Networks*, *163*, 103600.
[19] Tekchandani, P., Bisht, A., Das, A. K., Kumar, N., Karuppiah, M., Vijayakumar, P., & Park, Y. (2024). Blockchain-Enabled Secure Collaborative Model Learning using Differential Privacy for IoT-Based Big Data Analytics. *IEEE Transactions on Big Data*.
[20] Alahmari, S., Alshardan, A., Al-Wesabi, F. N., Sorour, S., Alghushairy, O., Alsini, R., ... & Al Duhayyim, M. (2025). A decentralized and privacy-preserving framework for electronic health records using blockchain. *Alexandria Engineering Journal*, *126*, 196-203.
[21] Maheshwari, V., & Prasanna, M. (2025). Privacy-preserving authentication for 5G healthcare with HBZKP: Hierarchical blockchain-based zero knowledge proof for secure edge devices. *Ain Shams Engineering Journal*, *16*(8), 103463.

Biographies

Dr. Santosh Reddy Addula, SMIEEE, currently works as a researcher at the Department of Information Technology at the University of the Cumberlands. His research focuses on Artificial Intelligence, Machine Learning, IoT, Cybersecurity, Blockchain, Cloud Computing, Automation and Robotics, Finance, IT Healthcare and Supply Chain Management. Santosh is dedicated to advancing knowledge and developing innovative solutions in these fields. He has demonstrated expertise across multiple domains. Santosh is an innovator with a strong portfolio of patents and has significantly contributed to academic research through his articles as an author and co-author. Additionally, he serves as a reviewer for esteemed journals, reflecting his dedication to advancing knowledge and ensuring the quality of scholarly publications in his field. saddula5840@ucumberlands.edu

Dr. Aitizaz Ali received the master's degree in computer systems engineering (with distinction) from GIK Institute, Topi, Khyber Pakhtunkhwa, Pakistan, and the Ph.D. degree in cybersecurity and blockchain technology from the School of IT, Monash University Malaysia, Jaya, Malaysia. He is a Lecturer with the School of IT, UNITAR International University, Petaling Jaya, Malaysia. He is the author of several Journal papers and international Conferences. He has authored or coauthored more than 20 research papers, including in highquality journals. His research interests include blockchain, cloud Ccomputing, cybersecurity, cryptography, deep learning, AI, and healthcare systems. Moreover. He was the Reviewer of IEEE Internet of Things Journal, IEEE Transactions on Network Science and Engineering, IEEE Access, IET, and Human-centric Computing and Information Sciences Journals for several years. aitizaz.ali@apu.edu.my