Received 16 January 2026; revised 2 March 2026; accepted 2 April 2026. Date of publication 7 April 2026; date of current version 8 May 2026.

Digital Object Identifier 10.1109/OJCOMS.2026.3681795

Blockchain Security Solution for a Dynamic Edge Computing Platform for Enhanced IIoT Application Performance

HAMEED HUSSAIN AL-MUBARAKIS[1,2] (Member, IEEE), AHMED JEDIDI[3], AND HAMID AL-RAWESHIDY[2] (Senior Member, IEEE)

[1]Computer Technology Department, Dammam College of Technology, Dammam 31472, Saudi Arabia
[2]Electronic and Electrical Engineering Department, Brunel University of London, UB8 3PH Uxbridge, U.K.
[3]Department of Computer Science, Applied Science University, East Al-Ekir, Kingdom of Bahrain

CORRESPONDING AUTHOR: H. H. AL-MUBARAK (Hameed.almubarak@brunel.ac.uk)

ABSTRACT In the context of the Internet of Things (IoT), the combined use of edge computing and blockchain technology is rapidly expanding. This approach improves performance, energy efficiency, storage management, and most importantly, security and privacy within IoT environments. IoT devices are also economically valuable across a range of industries, such as healthcare and manufacturing. However, because of their limited resources, energy constraints, and heightened vulnerability to intrusions, IoT devices and especially mobile IoT devices that move between networks face significant security challenges. Traditional security methods often become ineffective as the volume of data generated by mobile IoT devices continues to grow, which means that users become increasingly exposed to risks. To address these challenges, we propose a new method that integrates blockchain, edge computing, and mobile IoT devices. This method is known as the Secure Edge Mobility Protocol (SEMP) and is designed specifically for mobile IoT devices operating within edge computing environments. In the SEMP framework, IoT devices are able to roam smoothly and securely between networks through the dynamic generation of secure cryptographic keys created using blockchain technology and based on a modified PoAh protocol. This key generation mechanism strengthens device security while also improving system performance and energy consumption. The proposed SEMP architecture uses a decentralised structure, strong consensus mechanisms, and advanced encryption techniques that are suitable for resource-constrained mobile IoT devices. SEMP maintains high standards of privacy and performance for industrial IoT applications. It is implemented and rigorously tested under a wide range of realistic conditions. The results show significant improvements in security, robustness, scalability, and energy efficiency.

INDEX TERMS Blockchain, edge computing, Internet of Things, IIoT mobile devices, security.

I. INTRODUCTION

TODAY,, BC is crucial in situations involving edge computing (EC) and IoT devices; this prevents changes to the chain code, which is shared, copied, and synchronised by multiple parties [1], including edge servers (ESs). Furthermore, BC maintains secure and stable data exchange across EC and IoT devices, where cooperation among multiple parties is required, by strengthening trust between nodes and supporting efficient transaction processing. Although BC can provide strong transaction integrity, it also introduces challenges related to latency [4], [5] and energy consumption. EC offers benefits that can lessen these problems. Thus, combining BC technology with the processing power of EC services has become a viable way to improve security and privacy [6]. When combined with EC, BC can enhance traceability, transparency, and overall security and privacy. As a result, both EC and BC technology have already been widely adopted [7], [8].

The integration of BC technology within EC and the Industrial IoT (IIoT) can further improve the security of this layer in a cloud architecture. Furthermore, integration offers significant benefits that can alleviate concerns about security

and privacy in IoT communication [8], [9]. However, as more organisations increase their usage of IoT devices and the number of users interacting with them grows, new challenges will emerge. This situation is likely to lead to a surge in data generation and higher energy consumption. The IIoT faces significant challenges, as it is a transformative technology that was created to improve industrial and business processes through the use of connected devices in production environments [8], [9], [11]. One primary issue is that these devices generate vast amounts of data, which continue to increase daily. In addition, when these devices move between networks with encryption (public and shared key), they can create vulnerabilities in the IoT environment, and increase energy consumption due to the use of encryption. This can lead to a loss of trust in IoT technology, which again raises the initial concern of security [10]. The techniques used to implement BC technology have consistently improved across various sectors, including finance, industry [8] and the security and privacy of medical health data [12]. We propose the implementation of a BC solution to enhance the security of moving IoT devices that generate large volumes of encrypted data. This approach aims to improve the deployment of IoT devices by focusing on encryption, energy efficiency, and scalability. The goal is to ensure high standards of security and performance for industrial IoT applications, integrating BC and EC to achieve better protection and efficiency. The remainder of this paper is organised as follows. Section II provides an overview of related work in the integration between BC technology and EC. Section III introduces the proposed network model. Section IV presents some simulations' results and a discussion, and Section V contains a conclusion.

II. RELATED WORK

In this section, we will highlight several approaches that enhance data security for IoT and EC through the integration of BC technology. This integration can be applied in various sectors, including manufacturing and healthcare. As our approach combines BC with EC, we focus here on studies that have addressed issues related to data protection, enhanced edge efficiency, scalability, and improved overall performance. A challenge arises when transferring IoT devices between ESs with encrypted communication.

For example, one study [25] proposed a novel key management scheme that utilised BC technology for mobile EC (MEC), with the goal of ensuring secure group communication among mobile devices. The scheme involved generating lightweight key pairs for digital signatures and communication, broadcasting public keys to nearby users, and packaging all public keys into a block within the subnetwork's blockchain. The blockchain miner then distributed this block to other users, facilitating encrypted communication with peers by using the public keys stored on the BC. This approach enhanced security between IoT devices and MEC while reducing latency by employing lightweight key pairs. Another study presented a theoretical BC-edge framework that combined EC and BC technology for IIoT networks. BC was incorporated into each of the framework's three primary layers, which were IoT-edge networks (local networks), fog networks, and cloud networks (global networks). Key network components and their functions were described in the paper, including IoT nodes, edge nodes, local/private BC, and a centralised cloud. The researchers described how data moved between these layers and were processed. Parameters such as communication delay, computational power, and storage were considered in these simulations. Three components (low latency, security, scalability, and resource management) were identified as essential technological criteria for putting the framework into practice [13].

The authors of [14] used BC for processing power and instruction modelling, building on a similar approach from a prior health-block edge framework, called ''BlockEdge'' [14]. Using a lightweight BC with four resource-constrained IoT nodes and four local edge nodes, the suggested framework assessed performance at the local tier. Two fog/MEC nodes with greater computational power formed part of the access tier and were each linked to two local edge nodes. Using simulation characteristics such as processing capability, communication delay, BC instructions, and BC processing power, three scenarios (with and without BC pre-processing) were tested. The study used a simulation-based methodology to evaluate the framework's performance, with an emphasis on the effects of BC integration, by concentrating on four important metrics: latency, power consumption, total cost, and operational efficiency.

Kumar et al. [15] presented a novel method called Edge Blockchain Assisted Lightweight Privacy-Preserving Data Aggregation (EBDA). In order to implement a two-level data aggregation scheme and to ensure increased efficiency and security in smart grid data processing, this approach incorporated a three-layer architecture that made use of EC and BC. Better defence against network attacks was provided by the EBDA security system. It also lowered communication overhead and system processing costs, and could improve security and dependability by filtering false data and combining one-way hash chains and homomorphic Paillier encryption algorithms. EBDA was created to provide improved security, efficiency, and privacy in the processing of data from smart grids. Another study explored the use of an edge application module, called the Edgex Foundry framework, with a microservice architecture to address security and privacy challenges. A trusted edge platform was introduced that combined EC with BC networks. To ensure secure authentication, the platform leveraged the Hyperledger Fabric BC network. The authors evaluated the platform's usability and proposed a combination of EC, BC technology, and the Inter Planetary File System to develop a video surveillance system [8].

In order to improve data fusion and provide secure big data analysis for the IoT, the authors of [16] suggested a novel framework that combined BC technology with EC. They presented a technique that used node-level lightweight data fusion to offer safe, large data analytic services and effective data fusion for IoT applications. Since

a hierarchical fuzzy hashing technique was used to protect IoT data, data privacy was maintained while the validity and consistency of local and global models were ensured. In order to provide a reliable solution for data fusion and secure big data analysis in IoT contexts using node-level lightweight data fusion, the study introduced a framework that combined EC with BC. Hierarchical fuzzy hashing and lightweight data fusion techniques were found to work well in terms of improving security and lowering latency and data transmission. Since IoT data frequently contains sensitive information, privacy and security must be protected. The creation of TrustChain, a unique privacy-preserving BC especially for EC environments, was the main goal of the study in [17].

TrustChain sought to improve decentralised IoT operations, mitigate privacy vulnerabilities or data tampering concerns, and handle energy consumption difficulties. During communication, this system encrypted and anonymised sensitive data using methods such as zero-knowledge proofs. TrustChain undertook two primary tasks: firstly, by reducing redundant data storage, it improved transaction speeds by generating a historical record of the IoT system status, and secondly, it created trust attributes that made it possible to assess IoT devices, a crucial step in terms of guaranteeing the integrity and dependability of data transactions based on reputation, probability, and experience. Consequently, TrustChain was able to increase privacy and efficiency in IoT applications. Through the use of clustering and trust mechanisms, Panigrahi et al. developed CTB-PKI, a novel technique that was designed to increase the effective- ness of BC-based public key infrastructure (BC-PKI). Using variables such as validation time, trust levels, and response time, the system grouped participant nodes into clusters. To improve transaction security and narrow down the search space, a certificate authority (CA) was chosen inside each cluster. The use of node support evidence, the application of distributed trust models such as PeerTrust and PageRank, and trust calculation techniques depending on behavioural data and node operational status, were further contributions of this study. As a result, the CTB-PKI system significantly reduced the validation time by around 2.2% and the response time by roughly 38.5%. This suggested its possible use in BC 2.0 and 3.0 settings, which are mostly accomplished by cluster- based CA selection and trust assessment. The validation and response times and the amount of energy needed for different transactions were used to evaluate the system's performance [18].

Security is a crucial element in an IoT environment that involves vehicular EC networks (VECNets). A high level of responsiveness and large storage capacities are required to avoid leaks and threats. In order to solve issues such as data leakage and security hazards, researchers have suggested utilising smart contracts and consortium BC in VECNets to guarantee safe data sharing and storage. In particular, it presents two kinds of smart contracts: record pool smart contracts and local storage smart contracts. In order to gather trust value ratings and to enable a consensus process, these smart contracts are installed on dispersed edge nodes known as roadside units. Simulation results showed that the suggested concept using BC technology and incentive systems was able to improve the performance of vehicle networks [19].

Blockchain and IoT devices have also been used in agriculture. One notable example is the Intelligent Climate and Watering Agriculture System (ICWAS), which optimised water usage. To enhance security and address data privacy issues in IoT applications, researchers developed ICWAS by incorporating BC technology. This approach simplified secure watering schedules, ensured network security, and enabled rapid data analysis through the use of intelligent fuzzy logic. By leveraging BC technology, IoT devices can access information securely and communicate exclusively with trusted devices. In addition, this approach helped to ensure the safe tracking and traceability of system transactions. By implementing a decentralised storage strategy, vulnerabilities associated with central storage were minimised. IoT devices can efficiently store their data by connecting to network nodes. The findings of the study indicated that the proposed solution was scalable, effective, and secure, and provided safe access to trustworthy devices within a decentralised network [20]. To boost smart industrial productivity, the study in [21] investigated the integration of BC technology with EC and the IIoT. The researchers offered a novel BC-assisted data ex- change technique that ensured security in the IIoT domain by combining EC into BC nodes and employing smart contracts and a Proof of Authentication (PoAh) consensus mechanism. Blocks of transactions were disseminated for verification by geographically dependable nodes. Devices also used private keys to sign blocks, and public keys were exchanged for validation. The PoAh mechanism functioned in several different ways. Consequently, the proposed approach addressed significant challenges in IIoT scenarios and provided enhanced security, reduced latency, efficiency, and scalability. However, when there were more than 100 participating edge nodes, the performance of this approach drastically declined.

Through the use of PoAh, the authors of [22] aimed to advance BC applications in EC and IoT contexts. Their innovative consensus technique was created to improve IoT security. They also sought to overcome device resource limitations while safeguarding private and permissioned BCs. The emphasis of this approach was on creating, verifying, and appending blocks to the BC, although this gave rise to problems related to network broadcasting, device ledger storage, and validation energy usage. The study therefore, focused on the use of private BCs in IoT systems in view of their benefits, which include a low latency of about 3s in experiments, together with sustainability, scalability, and system security. In Tables 1 and 2, we summarise several strategies for securing EC and IoT environments, including approaches that distribute workloads across multiple nodes and use BC for secure data handling. We attempt

TABLE 1. Various techniques for securing the IoT environment by integration between EC and BC.

On.	Name of technique	Summary of technique	Advantages	Disadvantages	Aim	Ref.
1	MEC into WBN	IoT devices can upload transactions to a BC system by using ESs. A master leader must balance the needs of both clients and BC miners to manage the distributed nature of the BC system.	· High-level security · Immutability	· Requires high energy · Scalability · Latency	This method aims to achieve a high level of security and assesses its impact on system performance concerning confirmation delays.	[24]
2	Integrating UAVs into MEC	This approach showcases the most recent advancements in BC technology and federated learning. Unmanned aerial vehicles (UAVs) and edge computing technologies are combined in the UAV edge computing network. This affects the UAV EC network's federated learning phase. The next step is to integrate FL with BC to create security for UAV mobile EC. In the end, it illustrated UBFL's shortcomings and answers.	· Security and privacy · Immutability · Reliability · Low cost of communication · Resource allocation	· Limited battery capacity · Limited computing capabilities · Requires high energy · Scalability · Performance issues	A reliable, secure, and immutable solution is offered by the UBFL architecture for BC-enabled federated learning in UAV EC networks.	[27]
3	Integration of BC-based Internet of Edge model (BIoE)	In this method, the SC's responsibility is to transfer tasks to OpS for processing among ENs, allowing for the recording of related actions, energy expenses, and time consumption. ENs also have to finish jobs and determine how much time and energy they are using. OpS is used to perform the required Q-learning process to obtain an optimal Q-value function, which acts a future reward and is the optimal way to assign jobs to ENs and interact with SC on the BC. The BC system is composed of a number of blocks that store relevant data.	· An edge-based IoT system is effective · Preserves privacy · Ensures immutability	· Weak security · Energy cost · Scalability	The BIoE method, which employs BC techniques for job allocation, focuses on creating a privacy preserving plan for EC implementations in the IoT.	[28]
4	Integration of EB into a real-or-random (ROR) model	The IIoT device operates in a three-part environment: RFID readers gather information from tags that employ lightweight cryptography for IIoT authentication; EC links to the BC network and RFID readers to process data rapidly and in real time; and BC and RFID work together to increase system security.	· Enhanced security · Decentralisation · Immutability · Authentication	· Energy cost · Cost of computation	RFID tags and supply chain points can effectively and safely confirm each other's identities using this technique. EC is used to process data rapidly in real time with BC to make data decentralised and immutable.	[28]
5	ECBCM	ECBCM enhances nodes by consensus and supports them with the use of BC, making it easy to identify and replace corrupted nodes.	· Security · Scalability · Adaptability and efficiency of model with EC and BC	· Performance · Latency	The issues of efficiency, security, and adaptability with EC and BC were the main focus of this approach.	[6]
6	Novel BC-based key management scheme for MEC	Lightweight key pairs are generated by the system for communication and digital signatures. To enable encrypted communication and quick identity verification, so that mobile devices can effortlessly move across subnetworks, public keys are broadcast to peers and embedded into a block within the subnetwork BC.	· High security · Scalability · Low cost of communication	Requires high energy when the number of IoT devices in- creases (key update)	Mobile devices can easily move between subnetworks, and group communication is flexible and secure.	[25]
7	Edge-of-Things and BC (BEoT)	Through the use of BC, BEoT seeks to empower IoT applications to protect data privacy, improve access authentication, identify threats, and promote collaboration and trust in mobile EC.	· Security · Privacy · Low latency	· Requires high energy · Low capacity	BEoT is capable of faster, more effective data processing as well as secure, private data exchanges.	[26]
8	Edgex	Edge Foundry is a BC-based platform that manages heterogeneous forms of data, supports many protocols, and combines edge trust with IoT devices or apps. Hyperledger Fabric is used for access control for external requests and terminal identity authentication.	· Security · Privacy · Scalability · Real time(between ECs)	· Energy cost · Complex steps	This method seeks to accomplish access control and real-time security authentication of requests and services.	[8]
9	BC-edge framework (BlockEdge)	The primary components of this approach are data flows and process tracking across the various layers (local, fog, and global networks). Each of these layers is supported by BC.	· Security · Decentralisation · Low latency	· Requires high energy · Requires high capacity · Performance	Block Edge is searching for services that provide security, decentralized trust, minimal latency, and process tracking.	[13]
10	Integration of EC and BC in healthcare	The combination of BC and EC enhances collaboration and accountability in healthcare by ensuring secure, efficient, and decentralised data processing. BC modular design and the LSTM model provide trend forecasting, security, and anonymity, while EC relies on secure protocols such as TLS and SSH to maintain accountability. Together, they enable distributed edge devices to process data and make decisions effectively.	· Enhanced accountability and collaboration · Privacy and security · Immutability · Low latency	· Cost of energy · Capacity of data · Performance	This approach aims to achieve data privacy and security authentication of requests.	[23]
11	Integration of EC and BC for provision	The framework effectively addresses the challenges of network congestion and data security in IoT applications. By incorporating a node-level data reduction method and a hierarchical fuzzy hashing technique, the framework ensures efficient data fusion, secure machine learning model integrity, and robust performance, paving the way for scalable and reliable IoT deployments.	· Security · Privacy · Reduced amounts of data	· Scalability · Edge node load imbalance · Performance	This strategy reduces IoT data transmission while maintaining security by using a hierarchical fuzzy hashing method and a node-level lightweight data fusion mechanism.	[16]
12	BC-edge framework	The Health-BlockEdge framework consists of a basic BC system, four resource-constrained IoT devices, and four local edge nodes for the local layer. The access tier makes use of two fog or MEC nodes, each of which is connected to two local edge nodes and equipped with more potent CPUs. A cloud server situated on the core network oversees all of the main system operations. Simulations took into account a number of variables, including BC processing power and delay times.	· Latency · Computational power and local network access management · Security	· Scalability · Cost of energy · Performance	This approach aims to thoroughly evaluate the Health-Block Edge framework's performance, considering vital factors like speed, energy consumption, network requirements, total cost, and operational efficiency, regardless of whether BC is used.	[14]

to demonstrate some ways to protect the EC environment through the use of BC.

III. PROPOSED NETWORK MODEL

To create the proposed framework, the following assumptions were made about the network model and sensor nodes (SNs) to simplify the network model in the Encrypted ClientHello protocol:

1. Homogeneous SNs: All SNs are assumed to be homogeneous, with identical resources.
2. Equal Transmission Range: A data transmission range of 100 m is the same for all SNs.
3. Dead Node Consideration: SNs that have completely used up their energy are regarded as dead nodes, and are not allowed to participate in any activities.
4. Unique SN ID: The term ''SN ID'' refers to the distinct identification possessed by each SN.

TABLE 2. Comparison of techniques based on significant aspects in the IoT environment.

Type	Security	Low latency	Cost of energy	Scalability	Performance
Secure Edge Mobility Protocol (SEMP)	✓	✓	✓	✓	✓
BC-edge framework [34]	✓	✓	✗	✗	✗
BC-edge framework (BlockEdge) [31]	✓	✓	✗	✓	✗
Edge-of-Things and BC(BEoT) [12]	✓	✓	✗	✗	✓

FIGURE 1. Diagram showing how the Secure Edge Mobility Protocol (SEMP) is created by combining BC technology with EC.

5. Energy and Position Knowledge: Each SN is aware of its own energy level and present location. A global positioning system (GPS) or other position-determination tool is used to gather this data.
6. Pre-round Mobility: Before each round begins, SNs are mobile, but they do not move during each round. The movement of an SN is limited to a predetermined range and speed, and can take place either before or after the round begins.
7. Homogeneous ESs: All ESs are assumed to be homogeneous, meaning they possess identical resources.

We consider a distributed network based on EC as shown in figure 2. For each network, we deploy an ES connected to the cluster head (CH). None of the ESs communicates with the others. The SNs are also mobile, moving at a fixed speed within the network and between different networks. The CH is static and maintains a bidirectional connection with the ES. Lastly, the network is dynamic, meaning that nodes can be added or dropped during specific time intervals.

A. ENERGY MODEL

An SN model created especially for MWSNs is used in this study. The network's nodes are all homogenous, which means they have comparable traits. These nodes have limited energy resources, wireless communication capabilities, and sensing capabilities. Each node can also randomly travel at a defined speed, represented by the symbol ϑ, between locations. Ein, the initial energy, is the same for each node, and the following equation gives the energy consumption (1):

$$Econsumption = ET\ Rx + EMo + EPS \tag{1}$$

The energy of wireless communication, including during transmission and reception, is denoted by ETRx. ETRx denotes the energy of wireless communication

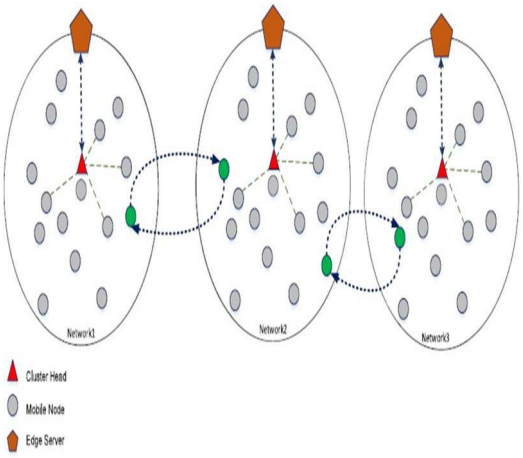


FIGURE 2. The network model and SNs.

for $\beta - bit$ data. The ETx and ERx, which represent transmission and reception, respectively, are calculated as shown in2:

$$ETx = (\vartheta t + Eamp * d2) * \beta \quad ERx = \vartheta r * \beta \tag{2}$$

where ϑt and ϑr represent the energy dissipated in sending and receiving one bit, respectively, and Eamp represents the energy used per unit time for the power amplifier during transmission. EMo represents the energy consumed in the mobility of the SN, and is calculated using equation 3:

$$E_{mobility} = E_{speed} * \frac{d}{\vartheta} \tag{3}$$

where E speed is the energy cost per second, d is the node's distance travelled, and ϑ is its speed. We represent the energy for processing and sensing as Eps, which consists of the energy used by the microcontroller and the sensor circuits, as shown in equation 4:

$$E_{ps} = P_{cpu} * t_{proc} + P_{sens} * t_{sens} \tag{4}$$

where:

- P_{cpu}: Power of processor
- t_{proc}: Processing time
- P_{sens}: Power of sensor hardware
- t_{sens}: Sensing duration

B. EDGE SERVER MODEL

Each ES is a self-contained computing node at the edge of a wireless sensor sub-network. Deployed per network slice, it connects to the slice's static CH via a wired or high bandwidth wireless link, creating a dedicated control and data channel.

The ES performs four core functions:

1. It authenticates incoming SNs using the PoAh process and issues or verifies edge-mobility tickets (EMTEs).
2. It executes real-time aggregation, feature extraction, and temporary caching so that only distilled data can be forwarded to the cloud or blockchain layer, thereby saving backhaul bandwidth.
3. It smoothly incorporates freshly arrived or departing SNs into the routing and security tables of the current round by updating its registry at predetermined intervals.
4. Each ES keeps its own routing, security, and trust databases, so that if one ES fails or is compromised, there is no effect on the network next to it.

Note: Each edge server runs the same software stack and has the same CPU, RAM, and non-volatile storage.

IV. SECURE EDGE MOBILITY PROTOCOL (SEMP)

To implement ES in the BC, each node generates a private and a shared key. In our SEMP protocol, based on PoAh, we enhance the handoff phase by issuing an EMT. Each data block in the ledger must trace back to a cryptographically verified device. The ES creates the EMT by hashing the node's local EdDSA key, network-signed certificate, trust score, and validity window after authentication. The node then uses the 256-bit EMT (Figure 2) for network switching, avoiding costly signature verification. The edge recalculates the hash and grants service if it matches. In dense mobile IoT setups with many short-lived connections, the EMT acts as a lightweight, self-expiring passport, reducing latency and CPU load while preserving PoAh's end-to-end integrity. Algorithm 1 outlines pseudocode for creating a local key to connect nodes to the correct network.

The EMT $Cr_{N(i)}$ is a signed certificate issued by network j for node i; this ties the node's unique identifier to the network's identity and verifies that this node is permitted to operate within the network for a specified validity period, as shown in equation 5.

$$Cr_{N(i)} \leftarrow H\left(SigNet_j \parallel NetId_j \parallel N_i\right) \tag{5}$$

To create a certificate, the network collects three important items: its network ID, the node ID, and the node's public key. It also adds selected start and end times. It then uses the network's digital signature to create a small, secure record that any ES in the same network can check on its own.

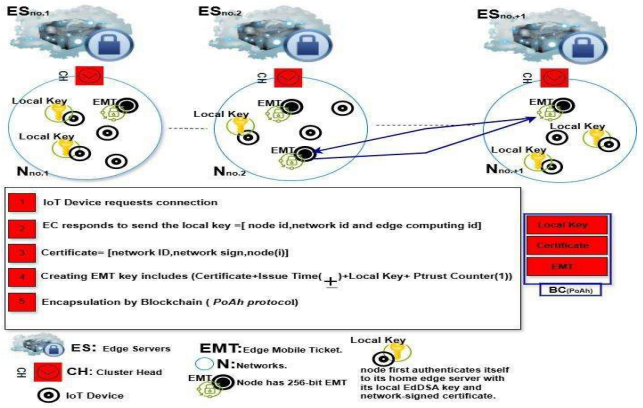


FIGURE 3. Steps taken by a node to generate the EMT and key.

Algorithm 1 Pseudocode for Local Key Generation

Input: $nodeID$, $node_{(x,y)}$, EC_j, Network ID
Output: local key, edge mobility ticket (EMT).
For $i \leftarrow 1$ **To** M //M is the total number of nodes in the WSN
For $j \leftarrow 1$ **To** K // K is the total number of the networks in the WSN
If $N(i)_{(x,y)} \subseteq Network(j)$ **Then** // $node\ (i)$ is the transmission region for network j
$N(i)_{(x,y)} \longleftrightarrow EC_j$//N(i) Connect to the edge computing node EC_j
$N\_localkey(i) \leftarrow$ $EdDSA[node\ id, network\ id\ and\ edge\ computing\ id]$//
Generate the local key
Generate the EMT
$Cr_{N(i)} \leftarrow certificate[network\ ID, network\ sign, node\ (i)]$//
Generate a certification from network j for node i
$EMT_{(i,j)} \leftarrow fct[Cr_{N(i)} + t_{iss} + t_{exp} + N_{localkey(i)} + Ptrust]$//
Combine the different parameters to generate the edge mobility ticket
End For
End For
Else
$N(i)_{(x,y)} \nleftrightarrow EC_j$// not valid connection to the network
End If
If $N(i)_{(x,y)} \longleftrightarrow EC_j$ **Then**
// Function IoT Node Submit to Blockchain:
$Payload \leftarrow \{Data \leftarrow Sensor\_Data\ Signature \leftarrow Sign(Data, localKey)$
Send Payload to Blockchain Node
End If
// Blockchain Node Verifies and Records
If Signature = valid **Then**

$Record\ Block \leftarrow$
$\{Device\_ID\ Time\ stamp\ Data\ Hash\_Pointer$

Append Block to Blockchain
Else
Reject Transaction
End For
End For

If the signature is correct and the time is still within the allowed period, the ES lets the node enter; otherwise, it blocks access.

$E\ MT\ (i, \mathrm{j})$ is the EMT issued by ES j to node i. It hashes together the node's current certificate $Cr\ N(i)$, the tickets

issue and expiry times, the node-edge local public key, and the edges' live trust score Ptrust. The resulting 256-bit digest acts as a compact ''passport'': whenever the node connects to another ES, it simply presents this value. The ES recomputes the digest from its own copies of the certificate, timestamps, key, and trust score; if the hash matches and the time window is still valid, the node is accepted instantly, and no signature verification or inter-edge queries are required, as shown in equation 6:

$$EMT_{(i,j)} \leftarrow H'[Cr_{N(i)} \parallel t_{iss} \parallel t_{exp} \parallel N\_localkey(i) \parallel Ptrust) \tag{6}$$

Algorithm 2 begins by examining each SN and network slice to determine whether a node's actual location is within a specific network area. If the node is inside that area, it must prove its identity: the ES verifies either the node's local public key at the edge or, if that fails, a valid EMT previously obtained by the node. If either credential is valid, the ES allows the connection, enhances the node's trust score, records the new EMT with a fresh timestamp, and initiates the data path. If neither credential is valid, the node is rejected immediately. An approved node uses its key to sign real-time sensor data and transmits this signed data to a BC validator. The validator verifies the signature; if correct, it creates a new block containing the device ID, timestamp, data, and a hash link. This process ensures that the data are permanently stored on the ledger, and guarantees three layers of security: location verification, credential authentication, and signature confirmation at the BC level.

This work assumes a standard adversarial model for mobile Industrial IoT environments, where attackers may attempt impersonation, replay, man-in-the-middle (MITM), Sybil attacks, or manipulation of trust values during network mobility. SEMP mitigates impersonation and Sybil attacks by binding each mobile IoT node to a cryptographically verifiable identity derived from its EdDSA key pair and a network-issued certificate, which must be validated through the Proof of Authentication (PoAh) consensus. Replay attacks are prevented through the use of time-bounded Edge Mobility Tickets (EMTs), which embed explicit issue and expiry timestamps and are invalidated once expired. MITM attacks are mitigated since EMTs and data submissions are always verified locally by the edge server through hash recomputation and signature validation, without reliance on external communication during handover.

The trust score (Ptrust) is protected against manipulation by restricting its update authority exclusively to authenticated edge servers participating in the PoAh consensus. Trust values are not self-reported by nodes and cannot be altered unilaterally; instead, they are computed based on verified behavioral history and recorded on the blockchain ledger, ensuring immutability and auditability. Any attempt to forge or reuse an EMT fails because the hash binds the certificate, trust score, public key, and validity window together. Consequently, even if an EMT is intercepted, it cannot be reused beyond its validity or transferred to another node.

Algorithm 2 Pseudocode of Node Connection to Edge Server

Input: $nodeID$, $node_{(x,y)}$, EC_j, Network ID
Output: node accepted, node rejected.
For $i \leftarrow 1$ **To** M //M is the total number of nodes in the WSN
For $j \leftarrow 1$ **To** K // K is the total number of networks in the WSN
If $N(i)_{(x,y)} \subseteq Network(j)$ **Then**//*node* (i) is the transmission region of the network(j)
  $N\ (i) \longrightarrow \{N\_localkey\ (i)\ EMT_{(i)} Node\ ID$
If $N\_localkey\ (i) = valid$ **Then**
  $N(i)_{(x,y)} \longleftrightarrow EC_j$// the node device N(i) $\in$ to network (j)
  $N\ (i)_{data} \leftarrow \{time\ issue\ Ptrust + 1 EMT_{(i,j)}$
Else If $EMT_{(i,j)} = valid$ **Then**
  $N(i)_{(x,y)} \longleftrightarrow EC_j$// the node device N(i) $\notin$ to network (j) but has a valid ticket
  $N\ (i)_{data} \leftarrow \{time\ issue\ Ptrust + 1$
Else
  $N(i)_{(x,y)} \nleftrightarrow EC_j$// not valid connection to the network
End If
If $N(i)_{(x,y)} \longleftrightarrow EC_j$ **Then**
  // Function IoT Node Submit to Blockchain:
  $Payload \leftarrow \{Data \leftarrow Sensor\_Data\ Signature \leftarrow Sign(Data, localKey)$

  Send Payload to Blockchain Node
End If
  // Blockchain Node Verifies and Records
If Signature = valid **Then**

$Record\ Block \leftarrow$
$\{Device\_ID\ Time\ stamp\ Data\ Hash\_Pointer$

  Append Block to Blockchain
  Else
  Reject Transaction
End For
End For

Through these mechanisms, SEMP provides resistance against common mobility-related attacks while maintaining low computational overhead suitable for resource-constrained IoT devices.

V. SIMULATION RESULTS AND DISCUSSION

This section details simulations of SEMP to evaluate its performance, scalability, and feasibility. The evaluation had two stages: (i) a Python-based environment estimated cryptographic key generation and processing latency, and (ii) a MATLAB simulation analysed the MWSN's lifetime under varying conditions. Simulations assessed the impact of node density, mobility, and network size on latency, demonstrating SEMP's ability to ensure low-latency security and efficient network performance over time.

For 200 rounds, mobile sensor nodes were tested using a four-edge grid and an eight-edge grid (Figure 3). After completing their initial ''KEY'' attachment with a full Ed25519 signature, 10%-50% of nodes roamed once per round. In the traditional baseline, average node-edge latency remained constant at ≈0.018 ms for the four-edge grid and ≈0.016 ms for the denser eight-edge grid, as each roaming required a new signature. With the SEMP protocol, where EMTs replaced new signatures, roaming latency dropped to ≈0.003 ms,

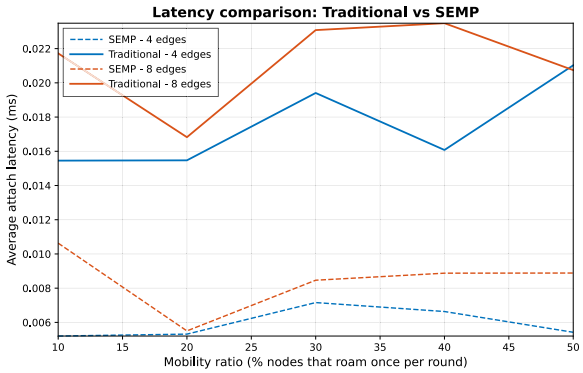


FIGURE 4. Latency times for four and eight edge servers.

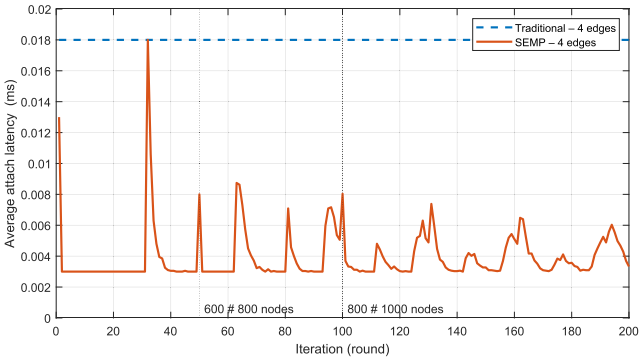


FIGURE 5. Latency time vs number of sensor nodes (600 to 1000).

lowering the overall average as mobility increased. SEMP reduced latency by ∼20% at 30% mobility and ∼40% at 50% mobility, regardless of grid size.

The ticket-based SEMP handover consistently outperformed the traditional "sign every time" method, especially in high-mobility scenarios, offering significant latency and energy savings. Lower energy consumption directly extends IoT device and system lifespans. Figure 4 shows that DTSA reduced average energy consumption by over 300%, enabling sustained system operation across cycles.

The IoT device itself has a significant impact on how much energy each device uses. It is also important to note that the security protocol used in the HST and ELT states consumes less energy than the conventional protocol when an IoT device is in these modes. Each occurrence of roaming necessitates a complete re-signature, with the same delay cost as the first attachment (0.018 ms). This is indicated by the dashed line in the curves, which represents the traditional method and stays nearly flat over the 200 rounds. The curve varies only slightly when new nodes join at rounds 50 and 100, since this cost is independent of the mobility pattern. The solid line represents the results from SEMP, which initially has the same latency as the traditional method, since each node completes a key attachment.

However, when the initial connection is made, the latency is dramatically reduced to the ticket-based roaming cost (0.003 ms). Due to fresh nodes making their first attachment, the SEMP curve exhibits small spikes at rounds 50 and 100 before settling down to a lower baseline.

The efficiency of reusing EMT rather than re-signing at each handover is shown by the gap between the two curves; with the parameters specified here and a 50% mobility rate, this leads to an average latency reduction of about 80–85%, with the magnitude of the benefit increasing with mobility.

Figure 5 compares network lifetimes for two methods, TRA and SEMP, with initial node counts of 600, 800, and 1000 in a setup with four ESs and 60% node mobility per round. The vertical axis shows the percentage of operational nodes over time, while the horizontal axis shows the number of rounds. TRA curves (dashed) drop faster due to the energy-intensive full sign-in process for each roaming event, resulting in earlier first node death (FND), half node death (HND), and last node death (LND).

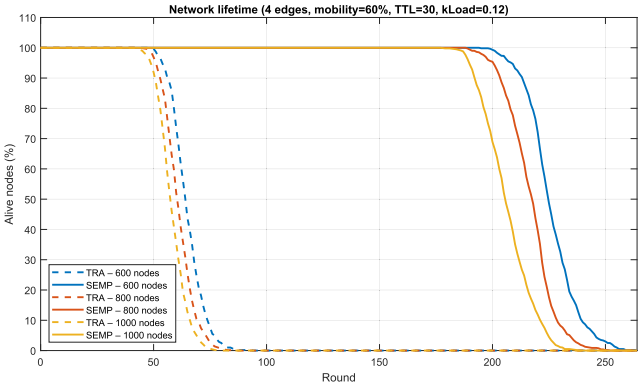


FIGURE 6. Network lifetime vs number of nodes (600, 800 and 1000).

SEMP curves (solid) last significantly longer, as roaming nodes reuse EMTs, which consume less energy than full sign-ins. The benefits of ticket reuse are more noticeable with larger networks, as energy savings accumulate over time. The slight differences between the 600, 800, and 1000-node curves for the same protocol are due to load scaling, where higher node counts slightly increase individual energy use, reducing overall network lifespan.

With a fixed network size of 600 nodes, the Figure 6 contrasts the network lifetimes of the TRA and SEMP protocols under three distinct mobility rates: 20%, 40%, and 60% of nodes roaming between ESs each round. Four ESs and a ticket validity (in SEMP) of 30 rounds are assumed in the configuration. Since each occurrence of roaming necessitates a complete key re-signature, which uses more energy, the TRA curves (dashed lines) decrease more quickly under all conditions. The lifespan in the TRA method decreases dramatically as the mobility rises from 20% to 60%, with LND occurring substantially sooner and FND occurring earlier. The SEMP curves (solid lines) indicate that nodes consistently last longer than their TRA counterparts. This is due to the reuse of EMTs. At a low mobility rate (20%), the difference between SEMP and TRA is moderate, but

TABLE 3. Simulation parameters.

Parameter	Value	Description
Number of ESs	4	Fixed grid configuration
Initial node counts	600, 800, 1000	Tested cohorts
Mobility rate	60%	Fraction of nodes roaming per round
Ticket TTL (SEMP)	30 rounds	EMT validity before renewal
Initial node energy (E_0)	40 units	Equal starting energy for all nodes
Key attachment energy (E_KEY)	1.00 unit	Cost for initial attachment or expired ticket
Roaming energy: TRA	1.00 unit × load scaling factor	Full re-signature cost per roam
Roaming energy: SEMP	0.25 units × load scaling factor	EMT reuse cost per roam
Load scaling factor (k_{Load})	0.12	Slightly increases energy cost for higher N_0
Lifetime metrics	FND, HND, LND recorded	First, half, and last node deaths

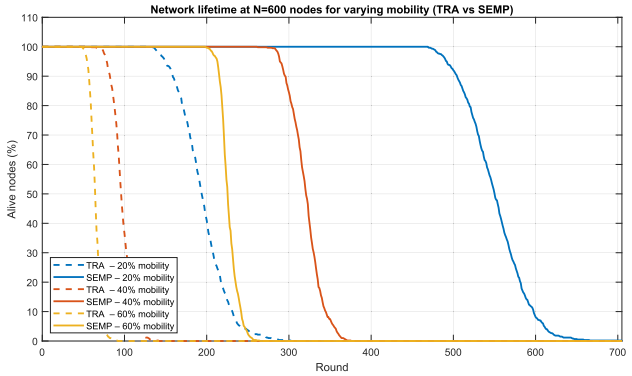


FIGURE 7. Network lifetime according to the mobility of SNs.

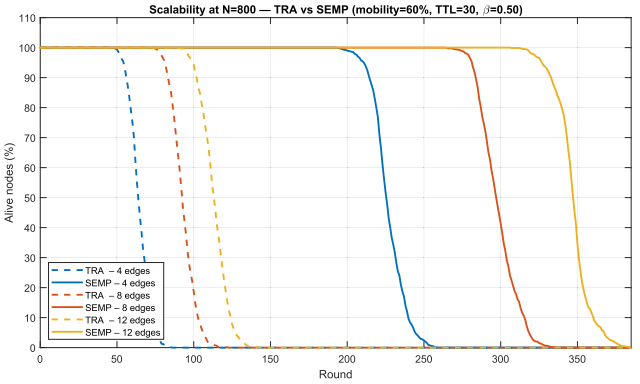


FIGURE 8. Network lifetime vs network scalability.

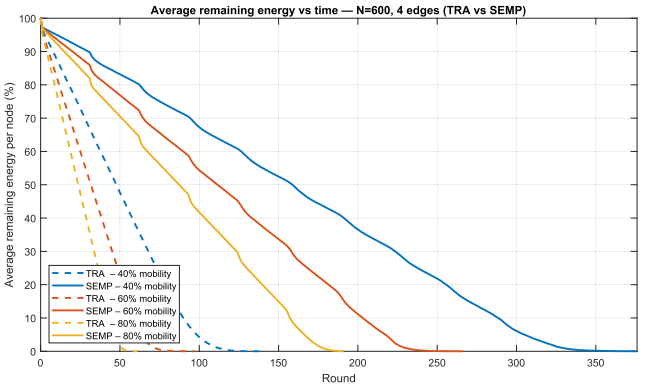


FIGURE 9. Average energy remaining for varying sensor mobility.

as mobility increases to 60%, the gap widens dramatically, with SEMP retaining a large proportion of active nodes for much longer before the final drop-off. This comparison demonstrates that SEMP not only extends the overall network lifetime but also scales better with higher mobility rates, while TRA suffers more severe performance degradation as the mobility increases.

Figure 7 compares network lifetimes for TRA and SEMP with 800 nodes under different setups of 4, 8, and 12 ESs, with a fixed mobility rate of 60%. The y-axis shows the percentage of surviving nodes over time (x-axis: rounds). Both protocols benefit from more ESs, as increased infrastructure reduces energy use during roaming. SEMP (solid lines) consistently outperforms TRA (dotted lines), with FND, HND, and LND occurring later. This scalability analysis highlights the importance of both protocol choice and network density in extending mobile IoT network lifetimes.

SEMP consistently outperforms TRA across all configurations because it uses EMTs, which significantly reduce the energy cost of roaming. The lifetime gap between SEMP and TRA remains noticeable, regardless of the number of edges, but the benefit of increasing the edge density is visible for both, especially when moving from four to 12 edges, as FND occurs significantly later.

For a network of 600 nodes connected to four ESs, Figure 8 shows the average energy left per node over time for three mobility rates: 40%, 60%, and 80% of nodes roaming per round. Each mobility rate includes two curves: a solid line for SEMP and a dotted line for TRA. The x-axis represents the number of rounds until all nodes are dead, while the y-axis shows the average battery percentage relative to initial energy. Since roaming requires energy-intensive key re-signatures, TRA curves drop faster across all mobility rates. Higher mobility (80%) accelerates energy consumption in TRA, reducing network lifespan. In contrast, SEMP exhibits slower energy loss, with curves consistently above TRA. This is due to EMTs, which reuse energy-efficient signatures, unlike the complete re-signature process in TRA. The energy gap between TRA and SEMP widens at higher mobility (e.g, 80%).

SEMP addresses key challenges for mobility IoT devices in EC environments, including security, energy, scalability, latency, and performance. Two components, Ptrust and EMTs, reduce latency and improve performance. Ptrust determines how many ESs trust a node, reducing scrutiny during network switches. EMTs allow nodes to reuse signatures,

minimising latency and energy consumption during roaming. This approach enhances scalability and reduces energy costs.

Simulations demonstrate that EMTs also achieve high security. Equation 5 shows how local keys are compared by ESs: matching keys result in acceptance, while mismatches lead to rejection. Additionally, data is encrypted using BC for encapsulation. This secure method, combined with EMTs, highlights their integral role in SEMP.

VI. CONCLUSION

Mobility in the IoT environment presents a big challenge for network performance in terms of energy consumption and security. In this paper, the urgent problems related to security, energy, scalability, and performance that affect mobility IoT devices operating in EC settings are successfully addressed by our proposed SEMP scheme. SEMP combines EC with BC technology and uses a modified PoAh protocol to generate cryptographic keys dynamically, ensuring safe and smooth network transitions for IoT devices. This novel method optimises energy economy and system performance while simultaneously improving the security, privacy, and scalability of IoT systems, which makes it especially appropriate for devices with limited resources. The resilience, flexibility, and usefulness of the proposed SEMP framework are demonstrated by extensive testing conducted under authentic industrial IoT scenarios, establishing it as a viable option for developing safe and effective IoT ecosystems. Future research will examine other improvements to scalability and the possible use of SEMP in various IoT-driven businesses.

REFERENCES

[1] Z. Xu, W. Liu, J. Huang, C. Yang, J. Lu, and H. Tan, "Artificial intelligence for securing IoT services in edge computing: A survey," *Secur. Commun. Netw.*, vol. 2020, pp. 1–13, Sep. 2020. [Online]. Available: https://www.hindawi.com/journals/scn/2020/8872586/

[2] K. Sha, T. A. Yang, W. Wei, and S. Davari, "A survey of edge computing-based designs for IoT security," *Digit. Commun. Netw.*, vol. 6, no. 2, pp. 195–202, May 2020, doi: 10.1016/j.dcan.2019.08.006.

[3] G. S. Aujla, A. Singh, M. Singh, S. Sharma, N. Kumar, and K.-K.-R. Choo, "BloCkEd: Blockchain-based secure data processing framework in edge envisioned V2X environment," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5850–5863, Jun. 2020, doi: 10.1109/TVT.2020.2972278.

[4] S. Xuan et al., "ECBCM: A prestige-based edge computing blockchain security consensus model," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 6, p. 4015, Jun. 2021, doi: 10.1002/ett.4015. [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1002/ett.4015.

[5] Z. Zhang, J. Feng, Q. Pei, L. Wang, and L. Ma, "Integration of communication and computing in blockchain-enabled multi-access edge computing systems," *China Commun.*, vol. 18, no. 12, pp. 297–314, Dec. 2021, doi: 10.23919/JCC.2021.12.019.

[6] H. Wu, K. Wolter, P. Jiao, Y. Deng, Y. Zhao, and M. Xu, "EEDTO: An energy-efficient dynamic task offloading algorithm for blockchain-enabled IoT-edge-cloud orchestrated computing," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2163–2176, Feb. 2021, doi: 10.1109/JIOT.2020.3033521.

[7] I. Handayani, D. Apriani, M. Mulyati, A. Rahmania Az Zahra, and N. A. Yusuf, "Enhancing security and privacy of patient data in healthcare: A SmartPLS analysis of blockchain technology implementation," *IAIC Trans. Sustain. Digit. Innov. (ITSDI)*, vol. 5, no. 1, pp. 8–17, Aug. 2023, doi: 10.34306/itsdi.v5i1.603. [Online]. Available: https://aptikom-

[8] Y. Wu, H.-N. Dai, and H. Wang, "Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in industry 4.0," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2300–2317, Feb. 2021, doi: 10.1109/JIOT.2020.3025916.

[9] J. Zhang et al., "A blockchain-based trusted edge platform in edge computing environment," *Sensors*, vol. 21, no. 6, p. 2126, Mar. 2021, doi: 10.3390/s21062126. [Online]. Available: https://www.mdpi.com/1424-

[10] T. Nguyen, H. Nguyen, and T. Nguyen Gia, "Exploring the integration of edge computing and blockchain IoT: Principles, architectures, security, and applications," *J. Netw. Comput. Appl.*, vol. 226, Jun. 2024, Art. no. 103884, doi: 10.1016/j.jnca.2024.103884. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1084804524000614.

[11] G. Wang et al., "Data-driven transient stability assessment using sparse PMU sampling and online self-check function," *CSEE J. Power Energy Syst.*, vol. 9, no. 3, pp. 910–920, Mar. 2023, doi: 10.17775/CSEEJPES.2021.05890.

[12] T. Qiu, J. Chi, X. Zhou, Z. Ning, M. Atiquzzaman, and D. O. Wu, "Edge computing in industrial Internet of Things: Architecture, advances and challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2462–2488, 4th Quart., 2020, doi: 10.1109/COMST.2020.3009103. [Online]. Available: https://ieeexplore.ieee.org/document/9139976/.

[13] T. Kumar, M. Ylianttia, and E. Harjula, "Securing edge services for future smart healthcare and industrial IoT applications," in *Proc. NOMS 2022-2022 IEEE/IFIP Netw. Oper. Manage. Symp.*, Budapest, Hungary, 2022, pp. 1–6, doi: 10.1109/NOMS54207.2022.9789900.

[14] Z. Wenhua, F. Qamar, T.-A.-N. Abdali, R. Hassan, S. T. A. Jafri, and Q. N. Nguyen, "Blockchain technology: Security issues, healthcare applications, challenges and future trends," *Electronics*, vol. 12, no. 3, p. 546, Jan. 2023, doi: 10.3390/electronics12030546. [Online]. Available: https://www.mdpi.com/2079-9292/12/3/546.

[15] T. Kumar et al., "BlockEdge: Blockchain-edge framework for industrial IoT networks," *IEEE Access*, vol. 8, pp. 154166–154185, 2020, doi: 10.1109/ACCESS.2020.3017891.

[16] M. Ejaz, T. Kumar, I. Kovacevic, M. Ylianttila, and E. Harjula, "Health-BlockEdge: Blockchain-edge framework for reliable low-latency digital healthcare applications," *Sensors*, vol. 21, no. 7, p. 2502, Apr. 2021, doi: 10.3390/s21072502.

[17] W. Lu, Z. Ren, J. Xu, and S. Chen, "Edge blockchain assisted lightweight privacy-preserving data aggregation for smart grid," *IEEE Trans. Netw. Service Manage.*, vol. 18, no. 2, pp. 1246–1259, Jun. 2021, doi: 10.1109/TNSM.2020.3048822.

[18] J. Dong, C. Song, T. Zhang, Y. Li, and H. Zheng, "Integration of edge computing and blockchain for provision of data fusion and secure big data analysis for Internet of Things," *Wireless Commun. Mobile Comput.*, vol. 2022, no. 1, Jan. 2022, Art. no. 9233267, doi: 10.1155/2022/9233267.

[19] U. Jayasinghe, G. M. Lee, Á. MacDermott, and W. S. Rhee, "TrustChain: A privacy preserving blockchain with edge computing," *Wireless Commun. Mobile Comput.*, vol. 2019, pp. 1–17, Jul. 2019, doi: 10.1155/2019/2014697.

[20] A. Panigrahi, A. K. Nayak, R. Paul, B. Sahu, and S. Kant, "CTB-PKI: Clustering and trust enabled blockchain based PKI system for efficient communication in P2P network," *IEEE Access*, vol. 10, pp. 124277–124290, 2022, doi: 10.1109/ACCESS.2022.3222807. [Online]. Available: https://ieeexplore.ieee.org/document/9954015/.

[21] S. Asaithambi et al., "A secure and trustworthy blockchain-assisted edge computing architecture for industrial Internet of Things," *Sci. Rep.*, vol. 15, 2025, Art. no. 15410, doi: 10.1038/s41598-025-00337-3.

[22] M. Firdaus and K.-H. Rhee, "On blockchain-enhanced secure data storage and sharing in vehicular edge computing networks," *Appl. Sci.*, vol. 11, no. 1, p. 414, Jan. 2021, doi: 10.3390/app11010414. [Online]. Available: https://www.mdpi.com/2076-3417/11/1/414.

[23] R. Kothari, "Integration of blockchain and edge computing in healthcare: Accountability and collaboration," *Transdisciplinary J. Eng. Sci.*, vol. 14, pp. 205–220, Aug. 2023, doi: 10.22545/2023/00230.

[24] W. Liu, B. Cao, and M. Peng, "Blockchain based offloading strategy: Incentive, effectiveness and security," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 12, pp. 3533–3546, Dec. 2022, doi: 10.1109/JSAC.2022.3213324.

[25] J. Li, J. Wu, L. Chen, J. Li, and S.-K. Lam, "Blockchain-based secure key management for mobile edge computing," *IEEE Trans. Mobile Comput.*, vol. 22, no. 1, pp. 100–114, Jan. 2023, doi: 10.1109/TMC.2021.3068717. [Online]. Available: https://ieeexplore.ieee.org/document/9387145/.

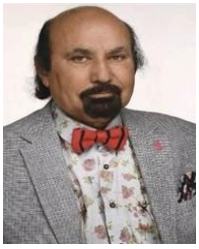
[26] B. Prabadevi et al., "Toward blockchain for edge-of-things: A new paradigm, opportunities, and future directions," *IEEE Internet Things Mag.*, vol. 4, no. 2, pp. 102–108, Jun. 2021, doi: 10.1109/IOTM.0001.2000191. [Online]. Available: https://ieeexplore.ieee.org/document/9409843/.

[27] C. Zhu, X. Zhu, J. Ren, and T. Qin, "Blockchain-enabled federated learning for UAV edge computing network: Issues and solutions," *IEEE Access*, vol. 10, pp. 56591–56610, 2022, doi: 10.1109/ACCESS.2022.3174865.

[28] V. Kumar and S. K. Das, "Enhancing security in IIoT: RFID authentication protocol for edge computing and blockchain-enabled supply chain," *Cyber Secur. Appl.*, vol. 3, Dec. 2025, Art. no. 100087.

HAMEED HUSSAIN AL-MUBARAKIS (Member, IEEE) received the Bachelor of Science degree in computer technology from Riyadh College of Technology, Saudi Arabia, in 2010, and the University of Kent, U.K., in 2020. He is currently pursuing the Ph.D. degree with the School of Electronic and Computer Engineering, Brunel University, London. He teaches numerous computer and network security courses, and he is interested in blockchain, artificial intelligence (AI), the Internet of Things (IoT), and edge computing, as well as security and privacy. Ha has 22 years of experience as an instructor at Dammam College of Technology, Dammam.

AHMED JEDIDI received the Ph.D. degree in computer engineering systems from the National School of Engineering of Sfax, University of Sfax, Tunisia, in 2012. He is currently the Dean of the College of Arts and Sciences, Applied Science University, Bahrain, and an Associate Professor with the Department of Computer Science. He is a member with the Computer and Embedded Systems Laboratory, University of Sfax. He has published numerous papers in international journals and conferences and brings more than ten years of teaching experience at universities in Tunisia and Saudi Arabia. His research interests include all-optical networks, embedded systems performance, optical network communications, and wireless sensor networks, with particular focus on the detection, localization, and estimation of crosstalk in all-optical networks. He is recognized for his academic leadership, commitment to quality in higher education, and dedication to program development, research, innovation, and student success.



HAMID AL-RAWESHIDY (Senior Member, IEEE) received the Ph.D. degree from the University of Strathclyde, Glasgow, U.K., in 1991. He was with the Space and Astronomy Research Center, Iraq; PerkinElmer, USA; Carl Zeiss, Germany; British Telecom, U.K.; Oxford University; Manchester Metropolitan University; and Kent University. He is currently a Professor of communications engineering. He is also the Group Leader of the Wireless Networks and Communications Group (WNCG) and the Director of PG studies (EEE) at Brunel University, London, U.K. He is the Co-Director of the Intelligent Digital Economy and Society (IDEAS), a new research center which is part of the Institute of Digital Futures (IDF). He is a Consultant and is involved in projects with several companies and operators, such as Vodafone, U.K.; Ericsson, Sweden; Andrew, USA; NEC, Japan; Nokia, Finland; Siemens, Germany; France Telecom, France; Thales, U.K. and France; Tekmar, Italy; Three; Samsung; and Viavi Solutions, actualizing several projects and publications with them. He was a Principal Investigator for several EPSRC projects and European projects, such as the MAGNET EU Project (IP) (2004–2008). He is also an External Examiner at Beijing University of Posts and Telecommunications (BUPT) and the Queen Mary University of London. He was an External Examiner for several M.Sc. communication courses at King's College London, from 2011 to 2016. He has published more than 450 journals and at conferences. His current research interests include 6G with AI and the IoT. He was an Editor of the first book *Radio Over Fiber Technologies for Mobile Communication Networks*. Specifically, he was an Editor with White Paper in communication and networking, which was utilized by the EU Commission for research. He has also contributed to several white papers. He was invited to give presentations at EU workshop and delivered two presentations on Networld2020, and was the Brunel representative for NetWorld2020.