Received: 11 September 2023 | Revised: 30 November 2023 | Accepted: 1 January 2024

DOI: 10.1111/exsy.13544

ORIGINAL ARTICLE

Expert Systems WILEY

A smart decentralized identifiable distributed ledger technology-based blockchain (DIDLT-BC) model for cloud-IoT security

Shitharth Selvarajan[1] | Achyut Shankar[2,3,4] | Mueen Uddin[5] | Abdullah Saleh Alqahtani[6] | Taher Al-Shehari[6] | Wattana Viriyasitavat[7]

[1]School of Built Environment, Engineering and Computing, Leeds Beckett University, Leeds, UK

[2]Department of Cyber Systems Engineering, WMG, University of Warwick, Coventry, UK

[3]Centre of Research Impact and Outreach, Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India

[4]School of Computer Science Engineering, Lovely Professional University, Phagwara, Punjab, India

[5]College of Computing and IT, University of Doha for Science and Technology, Doha, Qatar

[6]Computer Skills, Self-Development Skills Department, Deanship of Common First Year, King Saud University, Riyadh, Saudi Arabia

[7]Chulalongkorn Business School, Faculty of Commerce and Accountancy, Chulalongkorn University, Bangkok, Thailand

Correspondence
Shitharth Selvarajan, School of Built Environment, Engineering and Computing, Leeds Beckett University, LS1 3HE Leeds, UK.
Email: s.selvarajan@leedsbeckett.ac.uk

Funding information
Researchers Supporting Project number (RSPD2024R1034), King Saud University, Riyadh, Saudi Arabia., Grant/Award Number: RSPD2024R1034

Abstract

The most important and difficult challenge the digital society has recently faced is ensuring data privacy and security in cloud-based Internet of Things (IoT) technologies. As a result, many researchers believe that the blockchain's Distributed Ledger Technology (DLT) is a good choice for various clever applications. Nevertheless, it encountered constraints and difficulties with elevated computing expenses, temporal demands, operational intricacy, and diminished security. Therefore, the proposed work aims to develop a Decentralized Identifiable Distributed Ledger Technology-Blockchain (DIDLT-BC) framework that is intelligent and effective, requiring the least amount of computing complexity to ensure cloud IoT system safety. In this case, the Rabin algorithm produces the digital signature needed to start the transaction. The public and private keys are then created to verify the transactions. The block is then built using the DIDLT model, which includes the block header information, hash code, timestamp, nonce message, and transaction list. The primary purpose of the Blockchain Consent Algorithm (BCA) is to find solutions for numerous unreliable nodes with varying hash values. The novel contribution of this work is to incorporate the operations of Rabin digital data signature generation, DIDLT-based blockchain construction, and BCA algorithms for ensuring overall data security in IoT networks. With proper digital signature generation, key generation, blockchain construction and validation operations, secured data storage and retrieval are enabled in the cloud-IoT systems. By using this integrated DIDLT-BCA model, the security performance of the proposed system is greatly improved with 98% security, less execution time of up to 150 ms, and reduced mining time of up to 0.98 s.

KEYWORDS
blockchain, cloud, distributed ledger technology (DLT), security, internet of things (IoT), Rabin digital signature generation, Decentralized Systems

1 | INTRODUCTION

Blockchain is a kind of Distributed Ledger Technology (DLT) (Selvarajan, Manoharan, Iwendi, et al., 2023; Selvarajan, Manoharan, Shankar, et al., 2023; Uddin et al., 2023) mainly used to ensure data integrity and security properties, maintaining time series transactions. Here, the server update transactions are retained using the ledger technology and enforce each transaction's trust-based authentication/validation Field (Manoharan et al., 2023; Padmaja et al., 2021) processes. Due to this distributed nature, the blockchain methodology can efficiently avoid the risk of single-point failure because every networking node maintains a copy of each transaction data. So, it assures the integrity and reliability of transactions, which is one of the main reasons for using blockchain methodology in many smart application systems (Padmaja et al., 2021). Moreover, it also benefits IoT users, such as ensuring security (Manoharan et al., 2023; Selvarajan & Mouratidis, 2023) based on data validity, automatic reconciliation, proof-of-work, and increased transaction speed. Blockchain is a new and developing technology that cloud users can utilize to increase data safety and confidence while exporting and getting services from the cloud (Laghari et al., 2023; Vilas-Boas et al., 2023). Compared to centralized database security, Blockchain can offer enhanced security. Blockchain closely monitors the records safeguarded and connected to the preceding block via a cryptographic hash function. A distributed ledger that can record transactions and thwart manipulation is called a blockchain and is usually controlled via peer-to-peer networks that are intended to prevent tampering by the uninvited party. Blockchain technology can offer security comparable to central database data storage (Khan et al., 2023; Rahman et al., 2023). Attacks and harm to data storage can be avoided from a management perspective. Because of its transparent feature, the Blockchain can offer data transparency when data disclosure is necessary. Owing to these advantages, it can be applied in various contexts, such as financial services and IoT, and its uses are anticipated to grow. Because cloud computing is efficient and readily available, it has been implemented in numerous IT systems. Furthermore, cloud safety and privacy issues have been examined for critical security elements. The blockchain technologies (Yao et al., 2019) are categorized into the types of the public blockchain (permissions limited) and private (granting permission), in which the public model is available to all IoT users. But it has the challenges of control evolution, lack of scalability and regulations. The typical structure of the blockchain model is shown in Figure 1, which holds the Distributed Ledger Technology (DLT) (Aluvalu et al., 2021; Kamran et al., 2020), open architecture, smart contracts, trust and security. The DLT is a digital system used to properly transaction details, and the ledgers do not have the central data storage servers (Shahid et al., 2020; Zhu et al., 2019). The main reason for using this technology is that it guarantees security by maintaining all records at each transaction (Akhtar et al., 2021; Cullen et al., 2021). No one can change the information if the transaction is authenticated as valid.

A distributed ledger, or a database, comprises several storage devices where data is copied. Each storage device in the ledger has identical privileges, and the system assumes that member nodes are present with malicious intents. With other storage devices, a distributed ledger can function even if one of its storage devices malfunctions or is rendered inaccessible. The storage devices are dispersed in architecture but are centralized to provide consistency. The term 'distributed ledger technology' refers to the technological platforms that enable the distributed storage of information and data in an irreversible and accessible ledger. It allows distributed ledgers to operate on arbitrary, possibly unreliable nodes. The DLT-blockchain methodology is extensively used in many smart application systems to ensure the security and privacy of data (Nakanishi et al., 2020; Rakovic et al., 2019). In the existing works, the different types of key generation, cryptographic and blockchain methodologies have been used for securing the cloud-IoT systems (Altun & Tavli, 2019; Zhang et al., 2020) against the adversaries. In most recent cryptosystems, the digital signature schemes are mainly used to verify the authenticity of users or transactions. Moreover, the blockchain methodology allows valid

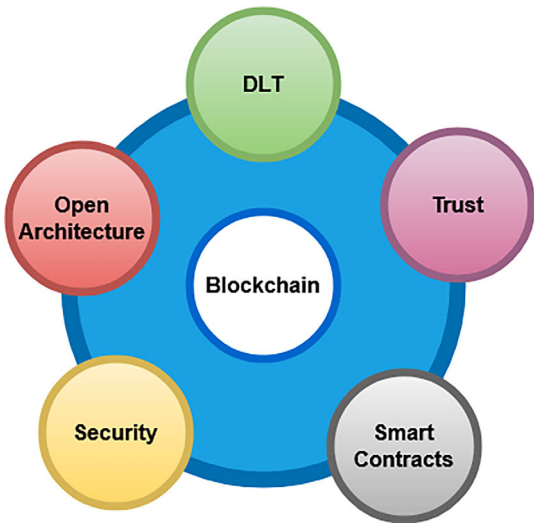

FIGURE 1 Blockchain model.

transactions (Sivaganesan, 2019) at the initial stage based on the digital signature generation and verification processes. The conventional works (Viriyasitavat et al., 2019) highly concentrate on developing a complete and secured blockchain architecture for IoT systems. Yet, it faced some challenges and problems associated with deploying blockchain models (Zhao et al., 2019), including complex computational operations for restricting the authenticated access, more energy consumption, lack of scalability, and immutable data. Hence, the proposed work intends to develop an intelligent blockchain model for increasing the security of IoT systems with reduced time and computational complexity. The IoT with cloud integration has attracted much attention in the past decade. Security is an increasingly challenging issue in the Cloud-IoT ecosystem as millions of sensors are linked together over the internet. A lot of research has gone into making cloud IoT security possible. However, the works have yet to demonstrate their effectiveness and security. The overhead is mainly raised by centralized authentication and intricate encryption protocols, regardless of low-level security. To address the security issue, this study suggests a unique Decentralized Identifiable Distributed Ledger Technology-Blockchain (DIDLT-BC) scheme best suited for resource-constrained IoT environments. The primary objectives of the proposed methodology are as follows:

- A blockchain methodology built on the Rabin digital signature guarantees the security of cloud-integrated Internet of Things applications.
- To ensure data security attributes, including privacy, confidentiality, safety, and integrity, by utilizing a blockchain-based security framework that requires less time and computational complexity.
- Hypothetical and security studies have been carried out to verify the effectiveness and safety of the suggested scheme.
- The Blockchain Consent Algorithm (BCA) is implemented to achieve outstanding dependability and security features.
- Several evaluation metrics, including time, throughput, latency, security level, and signature cost, have been verified and contrasted with the most recent state-of-the-art models to assess the performance of the suggested security model.

The system is initially established with IoT users, and generating a digital signature starts the transaction. This is the basis for using the private and public key pair for authentication. The Rabin digital signature-generating method initiates the transaction after the system configuration has been modelled. This public-key cryptography technique is mainly employed to improve data security between the parties involved in communication. It is lighter and faster than other cryptography algorithms, making it better suited for creating intelligent application systems. Building data blocks with the information of a block header, hash code, timestamp, nonce message, and transaction list is the primary goal of employing the DIDLT methodology. Blocks have been completed, and validation has been done to confirm that IoT users have accurately received their transactions. This architecture ensures the robust security field of IoT data against malevolent or aggressive users. The suggested DIDLT-BC paradigm has the following main benefits: minimal complexity, time consumption, high dependability, resilience, and guaranteed data security.

The rest of the units are structuralized as follows: Section 2 reviews the conventional key generation algorithms, cryptographic models, and blockchain technologies related to IoT security, which also investigates the benefits and limitations of the existing works. Section 3 describes the proposed methodology with its working flow model, architecture illustration, and theoretical analysis. Section 4 validates and compares the proposed method by using various evaluation indicators. Finally, the overall article is summarized with its future work in Section 5.

2 | RELATED WORKS

This section reviews the conventional blockchain methodologies used in various applications of cloud-IoT systems. Also, it discussed the importance and significant impacts of deploying the blockchain methodology with the problems faced by the existing works. Any application or request can be processed utilizing endless processors in a cloud centre, making cloud computing or the cloud a potent source of computational and storage resources. In a nutshell, the cloud has developed to enable devices to have low power, low computation, and small storage; because IoT devices are small and have limited computational, storage, and battery power, they use services from a third-party cloud to quickly complete their tasks. The significant issues of the cloud-IoT systems are listed below:

- Security & privacy
- Latency & scalability
- Cost & energy

Zhaofeng et al. (2020) implemented a blockchain-based decentralized authentication mechanism to increase Cloud-IoT security. The primary purpose of this work was to develop a reliable and secure IoT environment with fault tolerance capability. Also, the trust-based authentication strategy was deployed to ensure the security of systems, where the multiple data identity has been validated with the provision of digital certificates. Moreover, the Elliptic Curve Digital Signature Algorithm (ECDSA) has been utilized to validate the message's authenticity. The primary advantages of this work were that it ensured the security and stability of the IoT environment with reduced time complexity. Velmurugadass et al. (2021) employed an Elliptic Curve Integrated Encryption Scheme (ECIES) algorithm incorporated with the Harmony Search Optimization (HSO)

technique for increasing the security of IoT systems. This work mainly aims to develop a lightweight cryptographic methodology with the Logical Graph of Evidence (LGoE) to reduce response time and increase throughput and accuracy. The modules involved in this work are as follows: proper IoT user registration, authentication, data encryption, storage, blockchain management, and information mining. The different blockchain properties considered in this work were timestamp, target, nonce, Merkle root, and previous hash value.

Moreover, it addressed the security properties of access mechanisms, authentication ID, privacy, non-repudiation, and network security. However, this work limits the complex problems in computational operations and requires more response time to process the data. Erdem et al. (2019) constructed a new blockchain framework for increasing the security of the IoT environment with ensured trust, privacy, and protection. Here, the characteristics, benefits, and importance of using the blockchain methodology have been discussed. Typically, the primary purpose of using blockchain technology is to enable direct data transmission with satisfying reliability and data privacy. Moreover, this methodology has an increased ability to handle the problems of software updates, payments, and history tracking. Also, it examined the different types of IoT challenges associated with the deployment of blockchain methodology were also stated, which includes the following:

1. Diversity of device
2. Lack of skills
3. Processing power
4. Data storage
5. Response time
6. Lack of regulations

Moin et al. (2019) presented a comprehensive study for analysing the requirements and open issues of IoT systems, and it suggested a suitable solution based on the blockchain methodology. The IoT framework typically comprises three different layers: application, transmission, and perception. Here, the issues correlated to the IoT blockchain systems have been addressed, including data privacy, scalability, network speed, standards, security flaws, complexity, policy, and fork. In addition, the SWOT analysis was also conducted in this work to increase the security of IoT blockchain systems. Brotsis et al. (2019) suggested various blockchain solutions for protecting the IoT networks against intrusions and malicious users. This work mainly objects to construct the cyber-trust platform for identifying malicious activities using blockchain methodology.

Moreover, hyper ledger technology has been utilized to preserve the history of digital services. Rahman et al. (2020) developed a Distributed Blockchain methodology to enable secured data communication in IoT-SDN systems. The primary purpose of this article was to utilize the leading and advanced technology to ensure the privacy and security of smart condominium networks. In this model, the blockchain was mainly used to establish the secured data transaction by accurately detecting the attacks, where SDN controllers have effectively handled the IoT data traffic. Moreover, the cluster head selection process was performed based on the Euclidean distance computation, which supports improving the energy-saving and optimization operations. Yet, this work has the significant limitations of increased false positives, storage complexity, and time consumption.

Son and Kim (2019) constructed a new hyper ledger blockchain framework for increasing the security of the IoT environment. In this work, the firmware management system has been considered for application. The purpose of using blockchain methodology was to manage the state information of IoT devices and download the URLs to guarantee integrity. This architecture holds the entities of firmware provider and requestor, in which the provider constructs the internal network for transmitting the information to the IoT devices according to the request. Moreover, the hyper ledger model was utilized to analyse the transactions in the IoT device environment. The primary advantage of this system was that it efficiently prevents data falsification by enabling valid communication between the IoT devices and the network. Kouzinopoulos et al. (2018) object to strengthening the security of IoT systems by using the blockchain methodology, which provides an elegant solution to satisfy the security properties of integrity, authorization, and authentication.

Sisi and Souri (2021) deployed a blockchain methodology to enable secured data transmission and communication in IoT systems. The critical contribution of this work was to ensure the properties of data security and integrity by using the hybrid public-based blockchain methodologies. The blockchain has essential process integrity, immutability, anonymity, and privacy features. In addition to that, it enables a flexible framework for securing shared data information. Ryu et al. (2019) introduced a new blockchain-based decentralized framework for increasing IoT data integrity, transparency, and security. In this model, the Merkle tree hash value has been utilized to configure the blockchain, where the timestamp values were used to generate the blocks. The different types of participants involved in this framework were manufacturing, device user, investigator, and service provider. Still, this work limits the significant problems of increased time complexity and execution time, degrading the entire system's performance. Utilized an advanced DLT-based blockchain methodology to migrate the IoT devices securely. This framework includes the modules of a transaction initiated, broadcasting transaction, validation of marketing, and successful transaction. Here, the blockchain was constructed to verify the transaction based on authentication. Koshy et al. (2020) developed a sliding window architecture for increasing the security of IoT systems to increase IoT systems security with ensuring data privacy and validity. This work intends to construct a new blockchain model suitable for smart home applications, where real-time data streams have been generated to monitor the current status of information. Moreover, the block structure comprises the knowledge of block hash, block ID, timestamp, nonce, hash value, smart contract, and Enc data. Table 1 compares the existing blockchain methodologies with their advantages and disadvantages.

TABLE 1 Comparative analysis of the existing methodologies.

References	Methodology	Advantages	Disadvantages
Aluvalu et al. (2023) and Selvarajan, Srivastava, Khadidos, et al. (2023)	Blockchain Provenance (Block Pro)	It blocks the unregistered users, and efficiently preserves the integrity of data.	It requires an integrated solution for ensuring the security.
Rabie et al. (2023) and Thiruppathy Kesavan et al. (2023)	Firmware Over the Blockchain (FOTB)	It efficiently performs block verification using smart contract.	Complexity in computational operations.
Selvarajan et al. (2023) and Shitharth et al. (2023)	Lightweight Blockchain based Cybersecurity (LBC)	The framework is centralized in nature, increased throughput and reduced latency.	Increased bandwidth overhead, and energy consumption.
Kalid et al. (2023) and Lim et al. (2018)	ChainVeri—Blockchain Verification model	It enables the reliable data sharing between IoT devices, and better battery lifetime.	Increased resource consumption, and memory complexity.
Balaji et al. (2020) and Mao et al. (2023)	Simple Size Extensible (SSE) blockchain methodology	It minimized system irregularity, and computational latency.	Reduced level data security and trust.
Mahajan and Reddy (2023) and Xu et al. (2018)	Lightweight blockchain methodology	It attained an increased network throughput and reduced overhead.	Reduced efficiency and high packaging time.
Fan et al. (2021) and Issa et al. (2023)	Secured Blockchain Based Scheme (SBBS)	It ensured the secure data transmission with computational operations.	It lacks with the problems of inefficient data handling and storage overhead.

The research shows that traditional works have primarily concentrated on applying the blockchain technique to various applications to guarantee security. According to the analysis, classic works emphasize using blockchain in multiple applications to ensure security and secrecy. However, it is constrained by the common issues of:

- Excessive storage usage;
- Difficulty in building the blocks;
- Ineffective data handling;
- Lengthened processing times;
- Inadequate fault tolerance.

Therefore, the proposed work aims to apply a novel blockchain technique to protect IoT systems against damaging network attacks. To ensure secure data storage in cloud-IoT systems, the suggested system performs security operations in a digital signature generation, key generation, DLT-based blockchain modelling, and validation. The data is secured against hackers using simple mathematical procedures and little computational effort, thanks to the integration of DIDLT and BCA models.

3 | PROPOSED METHODOLOGY

This section describes the proposed DLT-based blockchain methodology to increase the security of cloud-integrated IoT systems. The main contribution of this work is to protect the data stored in cloud-IoT systems by using an advanced Decentralized, Identifiable Distributed Ledger Technology-based Blockchain (DIDLT-BC) model integrated with Rabin's digital signature generation algorithm. An optimization-based BCA is implemented to achieve high reliability in incorporating blockchain technology. The proposed system's working flow and architecture model are shown in Figures 2 and 3, respectively. This framework includes the following stages:

- Digital signature generation
- Key pair generation
- Block construction using DIDLT
- Block validation and formation

Initially, the system is initialized with the set of IoT users, and the transaction is initialized with the process of digital signature generation. Based on this, the authentication is performed with the private and public key pair. The main purpose of using the DIDLT methodology is to construct the blocks for data, which holds the information of block header, hash code, timestamp, nonce message, and transaction list. After

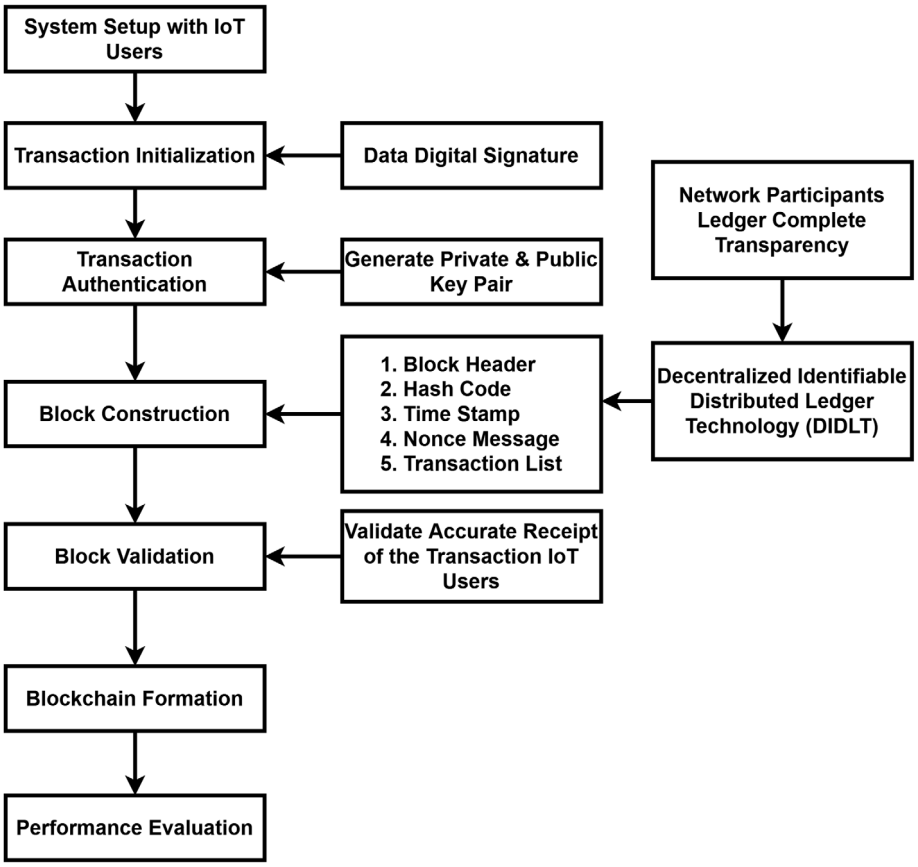

FIGURE 2 Working flow of the proposed decentralized identifiable distributed ledger technology-blockchain model.

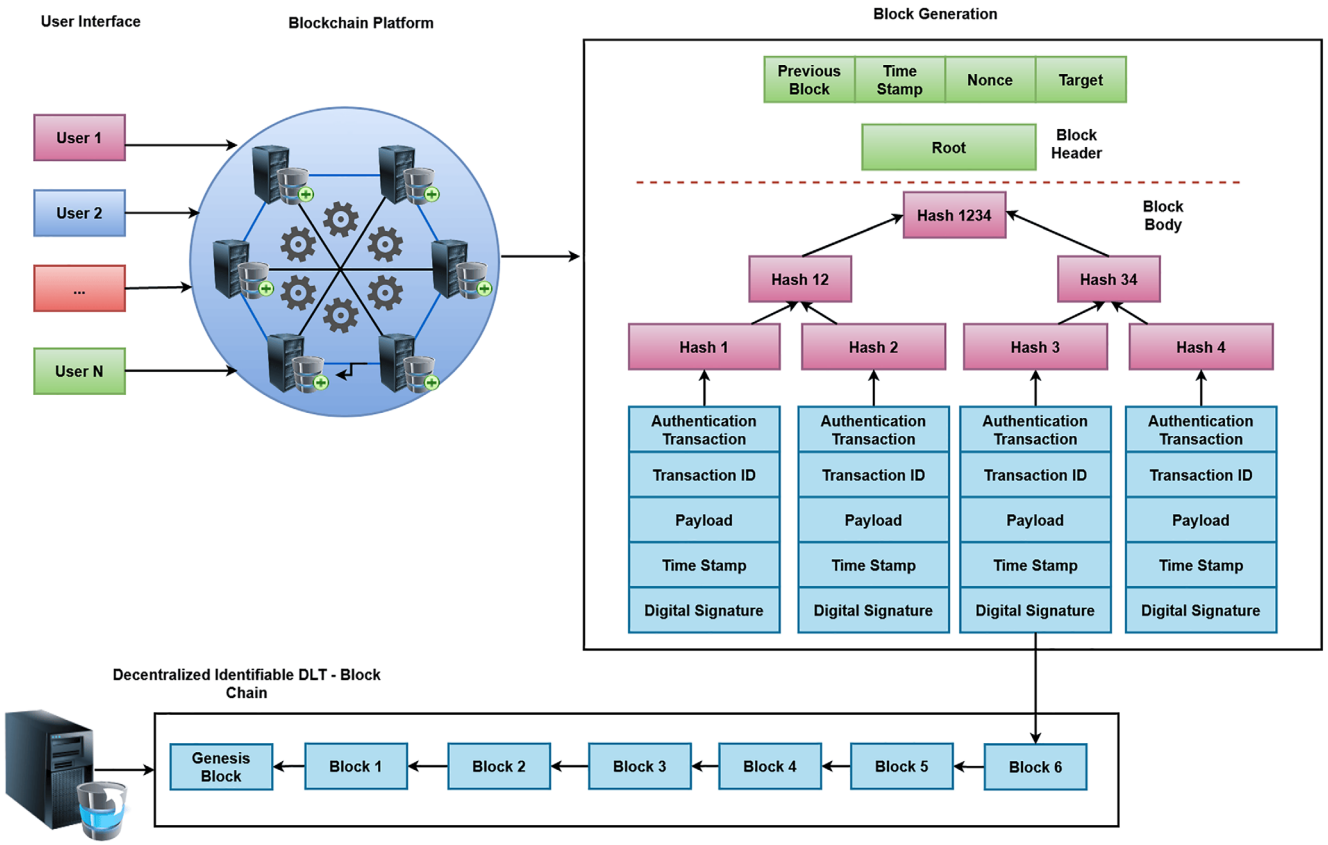

FIGURE 3 Architecture model of the proposed system.

completing blocks, the validation has been done to verify the accurate receipt of transaction IoT users. This framework ensures IoT data's strong security Field (Thiruppathy Kesavan et al., 2023) against malicious or attacking users. The primary advantages of using the proposed DIDLT-BC model are as follows: high reliability, robustness, minimized complexity, time consumption, and guaranteed data security.

In the proposed DIDLT-BC model, the transaction initialization is performed using the Rabin digital signature generation process. Consequently, the authentication process is carried out with the private and public key pair, which helps ensure secure data storage. After that, the DIDLT methodology is applied to construct the blocks for the data, which comprises the information of block header, hash code, timestamp, nonce message, and transaction list. Once the blocks are constructed, the data is stored in the cloud with blocks of information. When the receiver wants to access the data, the block is validated by verifying the transaction signature. In addition, properties such as reliability, security, and robustness are assured using BCA. When the process is run in a distributed mode in this system, the blockchain approach is mainly employed to have a single data value notation. Consequently, a Blockchain Consent Algorithm (BCA) has been proposed to provide high reliability when utilizing blockchain technology, offering methods for managing many unreliable nodes with varying hash values. Because blockchain technology lacks a central verification system, it is necessary to check each new block randomly using hash values. Consequently, BCA offers an extra benefit in this kind of role. When compared to the other existing models, the BCA has the unique characteristics of being simple to implement, having a low time for processing, and having less complexity.

3.1 | Rabin digital signature and key generation

The Rabin digital signature generating method initiates the transaction after the system configuration has been modelled. This type of public-key cryptography technique is mostly employed to improve data security between the parties involved in communication. It is lighter and faster than other cryptography algorithms, making it better suited for creating intelligent application systems. The following are the main benefits of applying this technique:

- It effectively prevents redundant message storage;
- No extra bits are needed;
- Processing performance is increased;
- Simplicity

Due to these factors, the proposed work intends to utilize the Rabin signature generation algorithm to increase data security. The list of symbols used in this system is illustrated with its corresponding description in Table 2.

Let consider, that the opponent outputs a message M, public key set G with n number of users, two different public keys $p_k^1, p_k^2 \in G$, which are all sent to the pretender. Then, the pretender randomly selects a bit $pk \in \{0,1\}$, and returns the Rabin signature as shown in the following format:

$$\rho = rabin(\mathsf{M}, R, s_k), \tag{1}$$

TABLE 2 Symbols and their description.

Notation	Description
I	Security parameters
$H(.)$	Hash value to user
s_k^i	User's private key
p_k^i	User's public key
M	Message
ρ	Rabin signature algorithm
ρ^*	Signature algorithm output at attacker side
m^*	Receiver message at the attacker
U_m	m-number of users
G	Group of public key set
$\mathbb{Z}$	The highest hash code
f	Maximum largest number
R	Generator of Q_1

where, ρ indicates the Rabin signature. Consequently, the safety parameter b is selected, a randomly generated large prime number $f > b$. Then, the base point Q is located on the elliptic curve, and Q_1 is a q-order cyclic addition with a large prime group. According to these, the output system parameters are generated as shown in below:

$$par = \left\{ q, Q, Q_1, R, H^0, H^1, H^2 \right\}. \tag{2}$$

The hash functions are generated based on the elliptic curve and integer field as represented in below:

$$H^0 : E(\beta) \rightarrow E(\beta), \tag{3}$$

$$H^1 : \{0,1\} \rightarrow \beta, \tag{4}$$

$$H^2 : \{0,1\}^* \times Q_1 \rightarrow \mathbb{Z}, \tag{5}$$

where, $E(.) \rightarrow$ *Elliptic curve*, and $\beta \rightarrow$ integer field. The user U_i $(1 \le i \le n)$ in the blockchain can randomly selects the hash value $\delta_i \in \mathbb{Z}$ for computing the public key. Then the user's public key is formed as p sub k to the i, script epsilon cap Q. Private key is included as $s_k^i = \delta_i \in \mathbb{Z}$. Finally, the generated public and private key pair are in the following form:

$$\vartheta \rightarrow \left(p_k^i, s_k^i\right). \tag{6}$$

After generating the keys, the transaction originators can select the public key set as $G = p_k^1, p_k^2, \ldots, p_k^m$, which comprises the group of public keys of the participating members.

3.2 | Block construction

Here, the set G does not have the public key p_k^t of the transaction originator, and the corresponding attributes values of G_i are generated for each public key concerning the following models:

$$G_i = \begin{cases} (a_i + c_i) * H^0\left(p_k^i\right) & if\ i = t \\ a_i * H^0\left(p_k^i\right) + (b_i + c_i) * \gamma_I & if\ i \neq t \end{cases}, \tag{7}$$

where, $a_i, b_i \& c_i$ are the coefficients obtained for every transaction, and γ_I indicates the signature image of the message calculated as follows:

$$\gamma_I = s_k^t * H^0\left(p_k^t\right), \tag{8}$$

where t indicates the transaction originators of signature, which is specifically used to avoid the double-spending attacks in the distributed ledger system. Moreover, the output of Rabin ρ is formed by grouping the following elements, where the value is randomly selected as $x \in \mathbb{Z}$ and the values are computed as shown below:

$$\hbar = H^2(\mathrm{M} \,||\, x), \tag{9}$$

$$v_i = \begin{cases} H^1\left(\hbar, G_1, G_2, \ldots, G_m\right) - \sum_{i=1}^{m} v_i & if\ i = t \\ a_i * H^0\left(p_k^i\right) + (b_i + c_i) * \gamma_I & if\ i \neq t \end{cases}, \tag{10}$$

$$w_i = \begin{cases} (a_i + b_i) - v_i * s_k^i & if\ i = t \\ a_i & if\ i \neq t \end{cases}, \tag{11}$$

where, M indicates the content of signature, and the Rabin signature of transaction originator t to the output message M as illustrated in below:

$$\rho = \left(\gamma_I, v_1, v_2, \ldots, v_t, \ldots, v_m, w_1, w_2, \ldots, w_t, \ldots, w_m\right). \tag{12}$$

During the verification process, any of the member having the Rabin signature's public key can verify the transaction signature ρ as shown in below:

$$\begin{cases} \tau_i = w_i * Q + v_i * p_k^i \\ \omega_i = w_i * H^0(p_k^i) + v_i * \gamma_I \end{cases}. \tag{13}$$

Then, the Equation (10) can be reformulated as shown in below:

$$\sum_{i=1}^{m} v_i = H^1(\hbar, \tau_1, \tau_2, ..., \tau_m, \omega_1, \omega_2, ..., \omega_t, ..., \omega_m). \tag{14}$$

Using Equation (13), the parameters tau sub i., omega sub i. are recomputed again to verify whether the formula is true. In this case, the signature γ_I has been confirmed for identifying whether it is legitimate or invalid. Consequently, the blockchain network's transaction set $\Ţ = \left(\Ţ^1, \Ţ^2, ..., \Ţ^m\right)$ for some time. The random numbers are estimated to satisfy the conditions for constructing the blocks that meet the confirming transactions' predefined requirements. Subsequently, the new block is broadcasted to the blockchain network, after it is successfully formed with the period. Based on the block construction procedure, the node confirms the legality of the new block. If it is legal, it can be added to the blockchain, and other nodes in the network should synchronize with the fresh blocks for receiving the next billing.

3.3 | Block validation

During this process, the verifier can validate the transaction signature ρ by using the following model:

$$\sum_{i=1}^{m} v_i = H^1(\hbar, \tau_1, \tau_2, ..., \tau_m, \omega_1, \omega_2, ..., \omega_t, ..., \omega_m). \tag{15}$$

If the condition is true, the validation is passed, when $i \neq t$, the renovation of τ_i, ω_i is as follows:

$$\tau_i = w_i * Q + v_i * p_k^i = a_i * Q + (b_i + c_i) * p_k^i, \tag{16}$$

$$\omega_i = w_i * H^0(p_k^i) + v_i * \gamma_I = a_i * H^0(p_k^i) + (b_i + c_i) * \gamma_I, \tag{17}$$

When $i = t$, the renovation of τ_i, ω_i is as follows:

$$\tau_i = \left[(a_i + b_i) - v_i * s_k^i\right] * Q + v_i * p_k^i, \tag{18}$$

It can be further reformulated into the following models:

$$\tau_i = a_i * Q + b_i * Q, \tag{19}$$

$$\omega_i = \left[(a_i + b_i) - v_i * s_k^i\right] * H^0(p_k^i) + v_i * s_k^t * H^0(p_k^t), \tag{20}$$

$$\omega_i = a_i * H^0(p_k^i) + b_i * H^0(p_k^i). \tag{21}$$

Based on the above relationship, the block is finally validated according to the Rabin signature scheme as represented in the following model:

$$H^1(\hbar, G_1, G_2, G_3, ...G_t, ..., G_m). \tag{22}$$

This kind of blockchain construction and validation model ensures an increased security of IoT systems.

3.4 | Blockchain Consent Algorithm (BCA)

In this system, the blockchain methodology is mainly used to have a single data value notation when the process is operated in distributed mode. Therefore, to achieve high reliability in incorporating blockchain technology, a Blockchain Consent Algorithm (BCA) has been introduced, thus providing solutions for operating multiple unreliable nodes with different hash values. Due to the lack of a central verification system in blockchain technology, it is essential to verify every new block with hash values randomly. Thus, BCA provides an additional advantage in this type of function. Moreover, high-security features can be enabled using BCA as the present state of operation can be easily monitored even if any unknown earls are existent in the proposed methodology. The local variables in BCA can be computed using the functional technique as given in below:

$$BC_i = \sum_{i=1}^{n} f(h_{in}), \tag{23}$$

where, h_{in} indicates the function of hash value variable as a local computation process. Also, it can be either represented for one process or even multiple process representations also it can be implemented. In the case of a single-stage process, there will be no delay during block transactions in the present state. However, if multiple processes are represented inside a single function, then the amount of uncertainty will be described in each block of transaction and it can be defined as follows,

$$D_i = \sum_{i=1}^{n} \frac{D_c(i) * t_i}{at_i}, \tag{24}$$

where, $D_c(i)$ denotes the corroboration delay of each block, t_i indicates total transaction that is processed per second, and at_i represents the average time period of each hash value that is processed per second. However, there is a high possibility that delay also occurs due to the slow computing power of each node as there is more number of target blocks, thus making the process to be more complex. Hence the delay can also be computed using by using the following model:

$$D_{\text{power}}(i) = \sum_{i=1}^{n} \frac{D_i}{CN_i}, \tag{25}$$

where, CN_i indicates the computational power of each node. The total delay calculated in Equation (37) will be given as input to solve the problem of complexity present at each node. Further, each hash function will have an arbitrary weight that creates some amount of delay in blockchain transactions which can be represented in analytical terms as shown below:

$$D_w(i) = \sum_{i=1}^{n} \frac{\vartheta_i}{\tau_{in}}, \tag{26}$$

where, ϑ_i, τ_{in} denotes cumulative function total and average weights. Even after many implementations, if the delay is much higher, the entire structure of the transaction log can be changed using the probability occurrence of variables which can be represented by using the following model:

$$P_{BC}(i) = \sum_{i=1}^{n} \frac{D_i}{D_w(i)} * (1 - D_w(i)), \tag{27}$$

Thus, the throughput of the above probability function can be represented as a maximization function as shown below:

$$\text{Throughput}_i = \sum_{i=1}^{n} \frac{\text{Total number of transactions}_{\text{in}}}{t_i - t_n}, \tag{28}$$

where, $t_i - t_n$ indicates the difference in time periods denoted in seconds. The flow of the consent algorithm is deliberated in Figure 4.

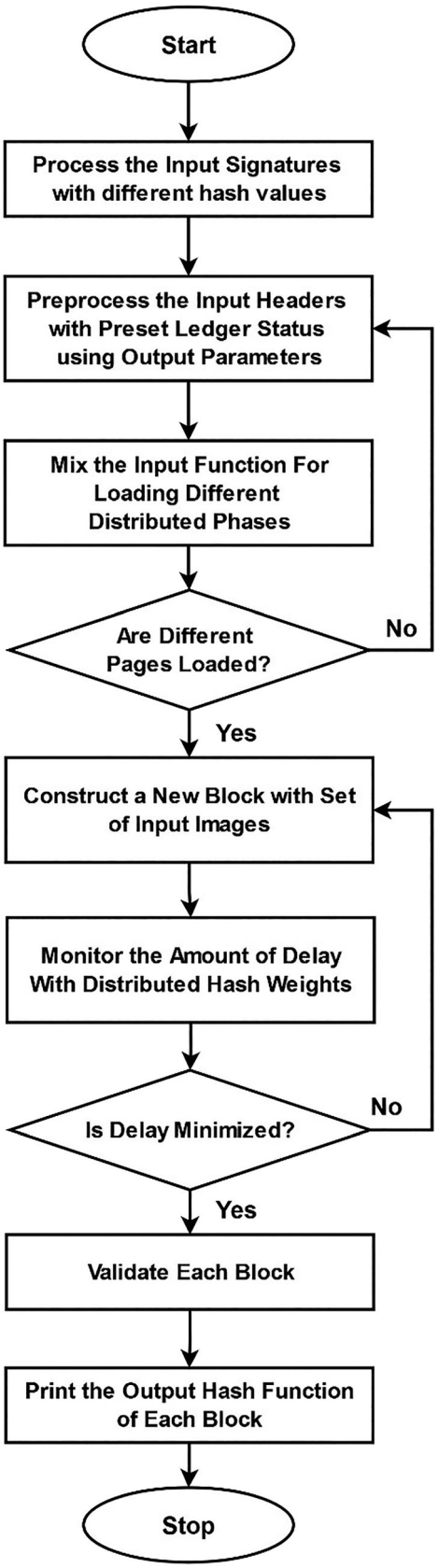

FIGURE 4 Steps involved in the blockchain transactions using Blockchain Consent Algorithm.

3.5 | Hypothetic analysis

Theorem 1. *In the Decentralized Identifiable Distributed Ledger Technology-based Blockchain (DIDLT-BC) system, the attacker can adaptively select the message to attack. Assume that, the Elliptic Curve based Rabin Signature (ECRS) algorithm is successfully processed with a valid polynomial-time ti. Also, the ECRS can be successfully solved with a non-negligible probability.*

Proof. If the pretender receives a random instance of the Rabin signature problem open $(P, v*P)$, the persistence is to estimate the value of v. The pretender sets a public key of the Signer U_m as shown in below:

$$p_k^{i*} = v*P. \tag{29}$$

Without loss of generality, it is assumed that all inquiries are different, and how the pretender responds to the attacker's query is determined.

Theorem 2. *The Rabin signature has considered as the unconditional secrecy of the signer; that is, for any algorithm $\tilde{A}$, any set of user sets $G = p_k^1, p_k^2, ..., p_k^m$ and a random $p_k^t \in G$,* the probability as represented below:

$$Pr\left[p_k^t = p_k^{t'}\right] is\, all\, \frac{1}{2}. \tag{30}$$

where, $\rho = (\gamma_l, v_1, v_2, ..., v_t, ..., v_m, w_1, w_2, ..., w_t, ..., w_m)$ is a rabin signature generated by p_k^t.

Proof.

1. The pretender performs initialization to calculate the system parameters and delivers them to the attacker.
2. Sender adaptively makes polynomial limited order respect to the Rabin signature query.
3. During the challenge phase, the adversary gives message M, the public key set G of m users, and two separate public keys $p_k^1, p_k^2 \in G$ to the pretender.
4. The pretender chooses a bit $p_k \in \{0,1\}$, at random, and the attacker receives the rabin signature as $= rabin(M, R, s_k)$
5. The receiver adaptively makes a polynomial limited order Rabin signature query.
6. Finally, the receiver outputs the bit as, $p_k \in \{0,1\}$.
7. The signature of the output is mysterious to any third party user, before the signer deliberately exposes all of the information himself. Then, the signer calculates the G_i values required to calculate the measures of $v_i$and w_i in the Rabin signature generator *rabin*. It is performed by randomly selecting the appropriate a_i and signer's private key, which is obtained by selecting $s_k^i = \delta_i \in \mathbb{Z}$ at random. It ensures that the signature ρ result is uniformly distributed in Q.
8. Based on the likelihood, the members outside the rabin can predict the actual signer is less than $\frac{1}{(m+1)}$ and, the members inside the Rabin can guess the actual signer is less than $\frac{1}{m}$. According to these conditions, the signature scheme in this work meets unconditional anonymity.

The following definitions can be used to understand the proceeding analysis, while others are unique to this work.

Definition 1. $(\hbar, \tau_1, \tau_2, ..., \tau_m, \omega_1, \omega_2, ..., \omega_t, ..., \omega_m)$, Let, consider $\hbar(t)$ be the number of times that the hash function is estimated, and φ_i is the empirical mean of hash for i^{th} user. This condition is defined as follows:

$$\varphi_i = \frac{\sum_{t=1}^{T} \tau_m(t)}{\omega_m}, \tag{31}$$

where, φ_i is the reward mean of hash value for the user i, $\tau_m(t)$ is the optimal hash value, and ω_m is the mean regret created by the beta distribution update. This value can be expanded based on the adversarial and its general proofs. Here, $the_i = |\varphi_i - \tau_m|$ is the remaining difference between the optimal and non-optimal hash values for each user i, and $\Phi_i(t)$ is a posterior distribution sample.

Definition 2. $(p_i \text{ and } q_i)$: p_i and q_i are two thresholds for $\Phi_i(t)$ where $\varphi_i < p_i < q_i < \tau_m$.

Definition 3. $\left(E_i^{\varphi}(t) \text{ and } E_i^{\Phi}(t)\right)$: Event $E_i^{\varphi}(t)$ occurs when $\varphi_i < p_i$ and $E_i^{\varphi}(t)$ occurs when $\Phi_i(t) \le q_i$.

Definition 4. (Distribution measurements): $D^{B}_{c,p}$ and $d^{B}_{c,p}$ denotes the binomial distribution's CDF and PMF respectively. Then, $D^{\beta}_{\alpha,\gamma}$ indicates the CDF of the beta distribution. In addition, the binomial and beta distributions are related based on the following model:

$$D^{\beta}_{\alpha,\gamma}(x) = 1 - D^{\beta}_{\alpha+\gamma-1}(\alpha+1). \tag{32}$$

Definition 5. (P_t): P_t is the hash value for the user with pull history, where $P_t = \{i(\varsigma), \tau_m(\varsigma), \varsigma = 1,...,t\}$ $i(\varsigma)$ is the user played for time ς, and $\tau_m(\varsigma)$ ς indicates the reward observed at time.

Definition 6. (Multiplicative Chernoff Bound): The multiplicative Chernoff Bound defines a bound for the tails of a distribution. This general bound can be applied to any random variable with $\varphi = \mathbb{E}(p)$.

$$\Pr(X \geq (1+\eta)\varphi) \leq \exp\left(\frac{-\varphi\eta^2}{3}\right). \tag{33}$$

Definition 7. (P_i): P_i is the maximum value that a change in reward for user i can take before, it is filtered out by $P = [(a_i + b_i) - v_i * \varphi]$. This value assumes that the reward and absolute change distributions are sub-Gaussian.

Definition 8. (Bi and Attack Strategy): Let, *Bi* is the budget, and an adversary influences reward for non-optimal users. Here, it is considered that the adversary selects the optimal attacking strategy based on LSI. For a general attack, the adversary influence is denoted as, $\gamma_i = \frac{\beta_i}{b_i(t-1)}$. For the LSI attack, the adversary influence is a massive influence over the user by using the accrued values $\alpha_i = \frac{\beta_i}{t}$. The adversary applies the influence by using the LSI strategy as, $\gamma_{i,t} = \beta_i - \sum_{k=1}^{t-1} \alpha_{i,k}$.

Rabin Signature Algorithm: Let consider the probability $\Pr(X \geq (1+\eta)\varphi)$ is obtained from the simple heuristic model denoted as random bisection. In this model, the relative length of the first prime factor of a random number is asymptotically obtained according to the random value ∂ that is uniformly distributed in [0, 1]. Then, it recursively proceeds with a random integer of relative size $1-\partial$. This model is used for computing a recurrence of $P(\mathfrak{v}) = \varepsilon(1/\mathfrak{v})$, where the asymptotic probability of all prime factors of a random value x is smaller than $x^{\mathfrak{v}}$. By using this model, ρ is considered as the Dickman's rho function defined for real $t \geq 0$ by the relation,

$$\varepsilon(t) = \begin{cases} 1 & \text{if } 0 < t < 1 \\ \varepsilon(r) - \int_r^t \frac{\varepsilon(s-1)}{s} ds & \text{if } r \leq t \leq r+1 \text{ for } r \in N \end{cases}. \tag{34}$$

For an $x^{\mathfrak{v}}-$smooth integer x, the relative length ∂ is selected based on the random bisection smaller than $\mathfrak{v}$, and the remaining integer of relative size $1-\partial$ is also $x^{\mathfrak{v}}$-smooth. Based on this, the following model can be obtained:

$$P(\mathfrak{v}) = \int_0^{\mathfrak{v}} P\left(\frac{\mathfrak{v}}{1-\partial}\right) d\partial. \tag{35}$$

Let, $Q(X \geq (1+\eta)\varphi)$ denotes the probability that a random integer z lies between 1 and X. Then, it divides the least common multiple of φ other random integers in the set of $\{1,...,X\}$. Let, $X' = \log_2 X, \varphi' = \log_2 \varphi$, and p_r be a prime factor of z with relative size $\partial\left(i.e. p_r = X^{\partial}\right)$. The probability ¢ divides the random integer in the set of in $\{1,...,X\}$ that is roughly ¢. Consequently, the probability Pr ¢ divides the least common multiple of ¢ random integers in $\{1,...,X\}$ is represented as follows:

$$Pr = 1 - \left(1 - \frac{1}{p_r}\right)^{\varphi} \cong 1 - \exp\left(\frac{-\varphi}{¢}\right) \text{ for large } ¢, \tag{36}$$

If $\partial \leq \varphi'/X'$, then $¢ \leq \varphi$ and consider $Pr = 1$. Otherwise, if $\partial \geq \varphi'/X'$ then $¢ \geq \varphi$ and, it is obtained as $Pr = \varphi/¢$.

$$Q(X \geq (1+\eta)\varphi) = \begin{cases} 1 & if\ x \leq \varphi \\ \int_0^{\varphi'/X'} Q(X \geq (1+\eta)\varphi)^{1-\partial}\ d\partial + \int_{\varphi'/X'}^{1} Q(X \geq (1+\eta)\varphi)^{1-\partial}\ \dfrac{\varphi}{x^{\partial}} & if\ x > \varphi \end{cases} \tag{37}$$

Let, $J(\alpha,\varphi') = Q(\varphi^{\alpha},\varphi)$, it is obtained as,

$$J(\alpha,\varphi') = \begin{cases} 1 & if\ x \leq \varphi \\ \frac{1}{\alpha}\int_0^{\frac{\varphi'}{X'}} J(\alpha-j,\varphi')\ dj + \int_{\frac{\varphi'}{X'}}^{1} (\alpha-j,\varphi')\ 2\text{^}(\varphi'(1-j))\ dj & if\ x > \varphi' \end{cases} \tag{38}$$

$$\frac{d^2J}{d\alpha^2}(\alpha-j,\varphi') = \frac{-\varphi' \log 2}{\alpha}, \tag{39}$$

$$J(\alpha-1,\varphi') + \left(\frac{1}{\alpha} + \varphi' log2\right)\frac{dJ}{d\alpha}(\alpha,\varphi'), \tag{40}$$

$J(\alpha,\varphi')$ for $\alpha \geq 0$ is considered as the solution with continuous derivative of the delay differential equation. Initial condition $J(\alpha,\varphi') = 1$ for $0 \leq \alpha \leq 1$. Here, a division-collision may occur if at least one integer divides the least common multiple of others. Also, it is assumed that those events are statistically independent, based on this the following model is obtained:

$$\Pr(X \geq (1+\eta)\varphi) \cong 1 + \left(1 - J\left(\frac{X'}{\varphi'},\varphi'\right)\right)^{\varphi}. \tag{41}$$

Table 3 compares the existing and proposed blockchain security models based on the parameters of the environment, multi-signature identity, fault tolerance capability, time complexity, security and reliability. According to this analysis, it is observed that the proposed model could effectively satisfy all the properties of the other techniques. Table 4 presents the generated hash values for the given strings.

4 | RESULTS AND DISCUSSION

This section validates and compares the results of the proposed blockchain model by using various evaluation metrics such as security, throughput, time, latency, and cost. The proposed methodology objects to ensure the properties of increased security, accuracy, and reduced complexity according to the user roles for enabling secured data access in IoT systems. As shown in Figure 5, the level of security is validated for the proposed model to demonstrate the high impact of security controls in the cloud-IoT environment. Also, the recent state-of-the-art security models (Sowmiya et al., 2021) have been considered for comparison, which include Linear Elliptical Curve Digital Signature (LECDS), Merkle Hashing Tree (MHT), Stochastic Diffusion Search (SDS), and Auth Privacy Chain. Based on this analysis, it is observed that the security level of the proposed DIDLT-BC model increased the level of security to 98%, when compared to the other methods.

Figure 6 validates the execution time of existing and proposed security models concerning varying bytes of information such as 1000 bytes, 3000 bytes, and 6000 bytes. In the proposed system, the decentralized identifiable Distributed Ledger Technology (DLT) based blockchain model constructs the secured and private communication channel for each IoT user, which helps to provide increased security for all data transactions. Hence, the DIDLT-BC technique overcomes the other existing methods with reduced execution time (i.e., lower time delay).

TABLE 3 Security analysis.

Methodology	Environment	Multi-signature identity	Fault tolerance	Time complexity	Security and reliability
PKP	Centralized	No	1	O(1)	Poor
CT	Centralized	No	1	O(1)	Poor
Duard et al.	Decentralized	No	$2f+1 \leq n$	O(n)	Medium
Sanda et al.	Decentralized	No	$2f+1 \leq n$	O(n)	Medium
Block Auth	Decentralized	Yes	$3f+1 \leq n$	$O(n^2)$	Strong
Proposed	Decentralized	Yes	$3f+1 \leq n$	$O(n^2)$	Very Strong

TABLE 4 Hash values for the given strings.

String	Hash value
Cryptography	**SHA-1**: BC9368B4CC142A10A1500474F14A59BCACCD6214
	SHA-256: FBC81B6E08FBC492693877ECB428A33420C38ADEA90CDEF1354BBA78E4B91B6B
	SHA-384: 4773242BF8E65FDDEA2B6F0BAF814BED6F20775C5D60851059501757FB0B1B07D3842065EB4EB7EBA51B89C02106DB65
	SHA-512: 6408678CF6097EDFA02279F53B36520AB1A84E55AE279106840EF02B0A534CDDF48812A974DF438044B126F067EC650AA609FCBD26D3FEF3443C39EBD5A4C3A4
	MD2: 0C599631391DE5EC08F070E01D55E655
	MD5: 8C8B95F84334ED1199ADAF8D07B80F94
'Data Security'	**SHA-1**: E624E2E960467E3CC06AB55D25F8DEF7289D6B92
	SHA-256: CDE4D6F144BA4C83CA832E299C3A987686FD2DB7AF5A8DB750835C371F91C804
	SHA-384: 1229B10DBDCF2F9615BB70767EA603709CA211A837A10EBC9253990B1C327CED85DDEC3639E7405FA0A7FEA0E4F027C5
	SHA-512: 93DCFF755F8C523835928ED16694F03C73390B3391814C2466E291F9930B640979095534AE5DA8AE9C17720C23BB8FC8BCD0394B7E52935DC17080BDEC481D22
	MD2: 656209F8FA2B564E97570416FECCCB1C
	MD5: 2147C43BA0211AAFA9D8F1BE2100BDEF

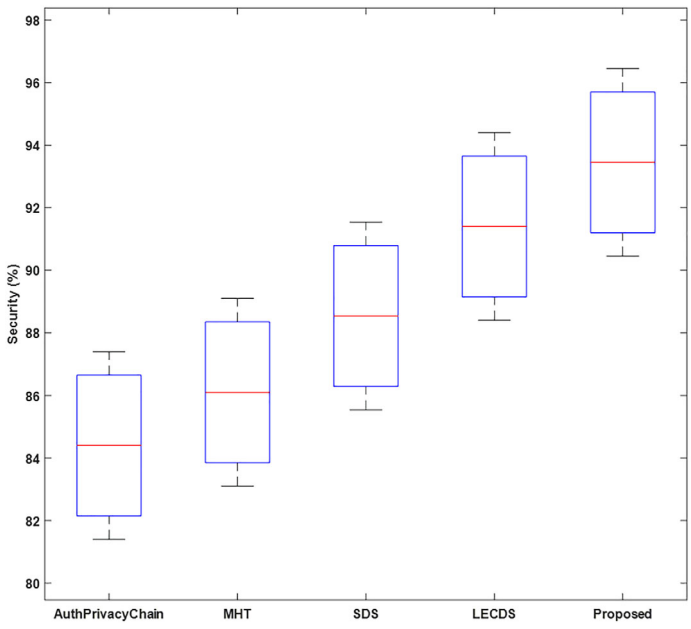

FIGURE 5 Analysis of security level (%).

As shown in Figure 7, the throughput rate is compared for both existing and proposed security mechanisms with respect to the number of transactions. The Rabin signature generation process could efficiently minimize the user searching time, which results in increased throughput. Compared to the existing techniques, the proposed DIDLT-BC could efficiently improve the throughput value for all data transactions.

Figure 8 compares the average latency of existing and proposed models concerning a varying number of transactions. As depicted in this analysis, the proposed DIDLT-BC provides a reduced latency value compared to the other techniques. Also, the proposed model takes 0.5 s for 25 data transactions, while the other methods have 0.6, 0.98, 1.22, and 0.7 s. From the evaluation, it is analysed that the proposed model's average latency is lower than other models. Consequently, Figures 9 and 10 validate the signature verification time of the existing RSA (Mazumdar & Ruj, 2019) and proposed Rabin signature generation schemes concerning a varying number of endorsers. Typically, the signature generation and

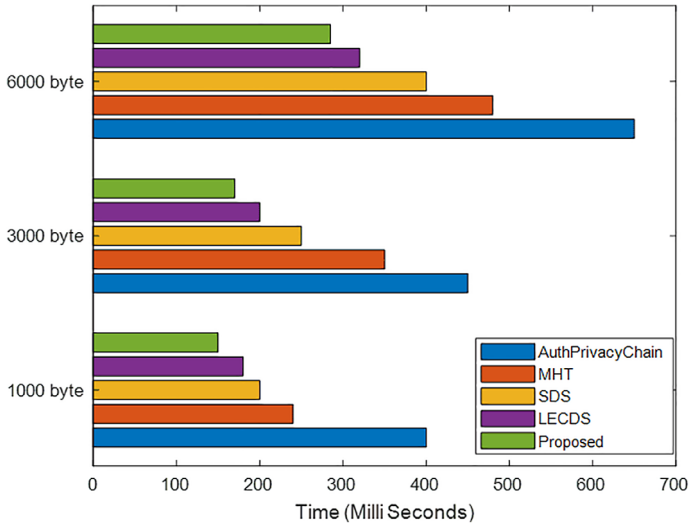

FIGURE 6 Execution time.

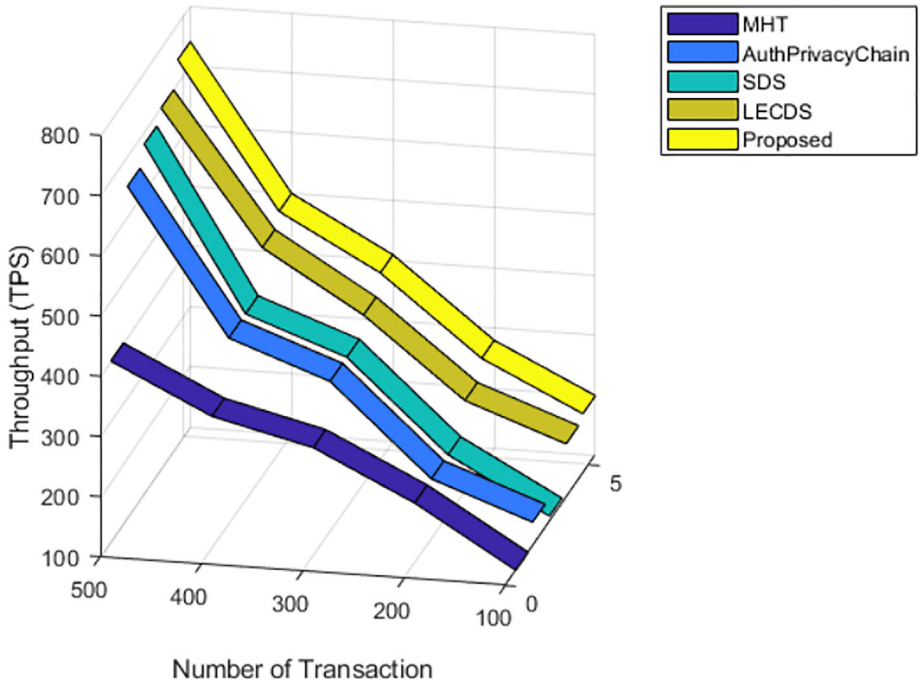

FIGURE 7 Throughput rate.

verification time are defined by the amount of time taken for generating and verifying the forged signatures before enabling the transactions. Also, every signer in the system can parallelly create the signature, which can be used to verify the single signer. Moreover, the signature generation and verification are sequentially performed to validate the signers. For this evaluation, the varying number of keys having different sizes are considered, including 1024, 2048, and 3027 bits. The review shows that the proposed Rabin digital signature scheme requires less signature generation and verification time than the RSA algorithm.

Figure 11 validates the mining time of the existing qTESLA + IPFS (Zhang et al., 2021) and proposed DIDLT-BC methodologies concerning varying block sizes. According to this analysis, it is observed that the mining time can be linearly increased with the change in block size. After constructing each block, the miner can validate the data transaction, which is sequential. From the evaluation, it is analysed that the mining time of the proposed model is lower than the existing qTESLA model for all sizes of blocks, which depicts the efficiency and improved performance of the proposed model. Figure 12 estimates the security level of existing (Li et al., 2021) RSA, ECC, and anti-quantum lattice and presents DIDLT-BC

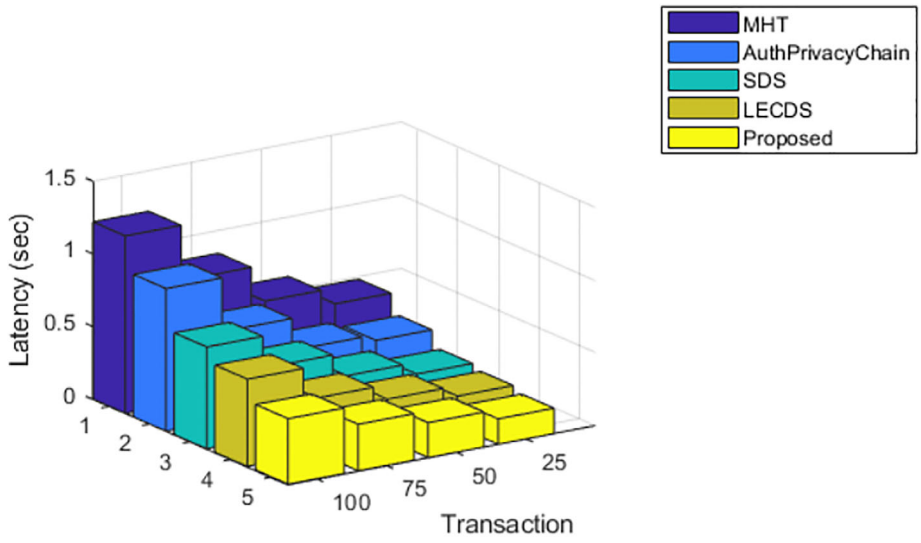

FIGURE 8 Latency.

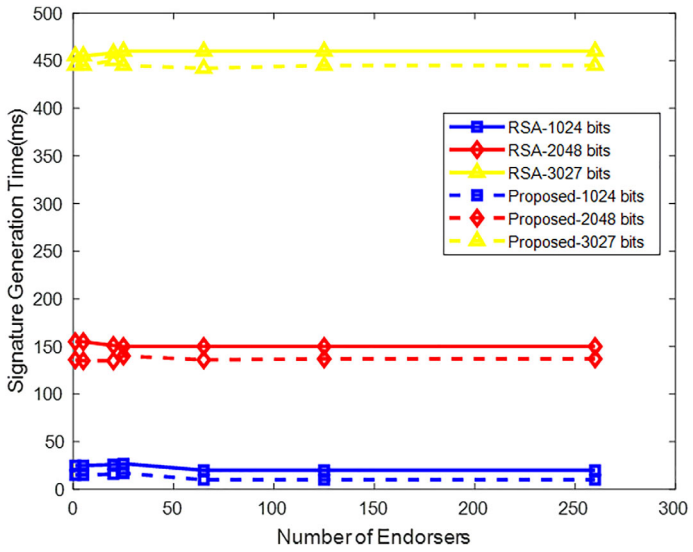

FIGURE 9 Signature generation time.

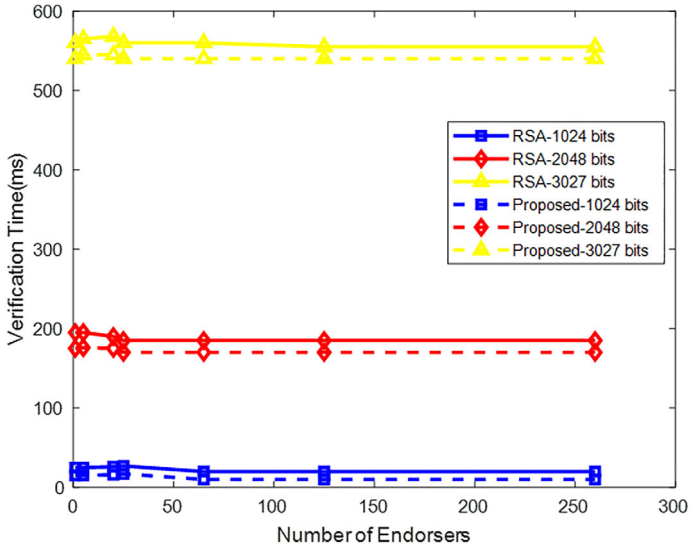

FIGURE 10 Verification time.

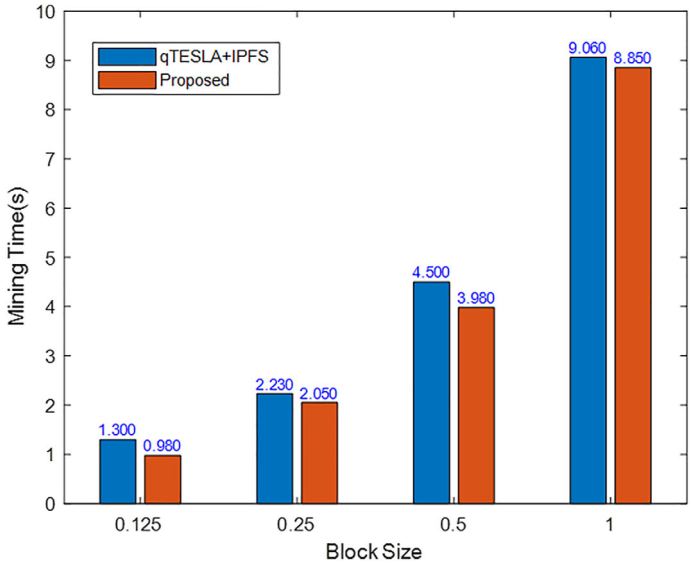

FIGURE 11 Mining time.

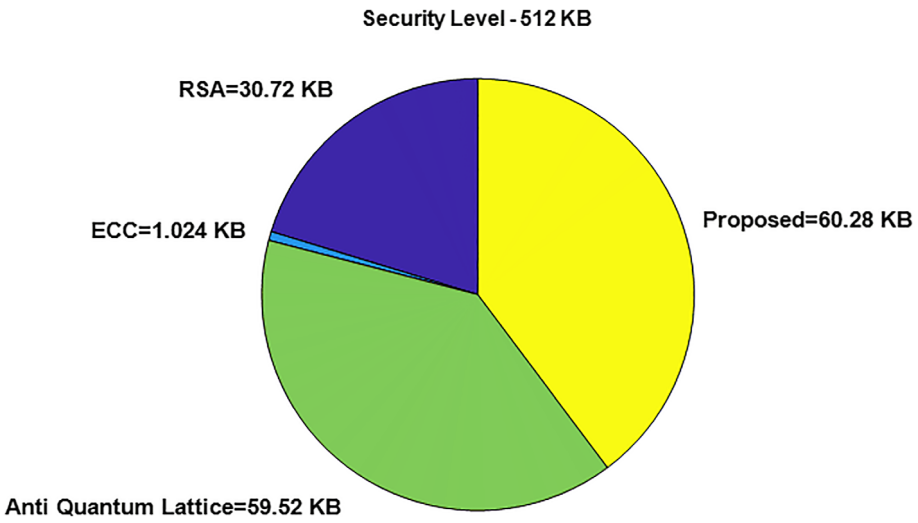

FIGURE 12 Security level.

models concerning the security of 512 KB. In this analysis, the security level is estimated based on the size of the signature, where the RSA is 30.72 KB, ECC is 1.024 KB, and anti-quantum lattice is 59.52 KB. Compared to these models, the proposed technique could efficiently increase the security level to 60.28 KB. Similarly, Table 5 compares the security level of existing and proposed cryptographic models concerning varying sizes of signatures in terms of KB. It also depicts that the proposed model outperforms the other techniques with an increased level of security concerning all sizes of signatures.

Figures 13–15 compares the signature verification cost, generation cost and total cost of existing (Liu et al., 2021) ECDSA, Zhangs' algorithm, ECDLP, and proposed DIDLT-BC models with respect to varying size of blocks in terms of bits. Compared to the other models, the signature generation of the proposed model is 0.97% less than existing models, and the verification cost is 0.1% less than the other models because the proposed scheme increases the security of IoT systems and efficiently minimizes the computational steps involved in the security operations.

Figure 16 validates the time and security level of the proposed model with respect to a varying number of transactions. Usually, the performance of the blockchain model entirely depends on the measures of time cost and security level, which determines how efficiently the blockchain model could secure the IoT systems against the adversaries. Here, the number of transactions has been considered for validating the measures of time and security.

Similar to that, Figure 17 estimates the time of proposed DIDLT-BC concerning varying block size and message size. According to the evaluations, it is observed that the time could be efficiently reduced with the increased level of security. Figure 18 shows the latency of the proposed model concerning the varying number of blocks and IoT users. The latency is also defined as the time delay of processing, which should be

TABLE 5 Security level versus signature size.

Techniques	Security level					
	80 KB	112 KB	128 KB	192 KB	256 KB	512 KB
RSA	1.024	2.048	3.072	70.68	15.36	30.72
ECC	0.16	0.224	0.256	0.384	0.512	1.024
Anti-Quantum Lattice	57.26	57.67	57.84	58.33	58.68	59.52
Proposed	60.13	60.67	61.11	60.35	61.47	60.28

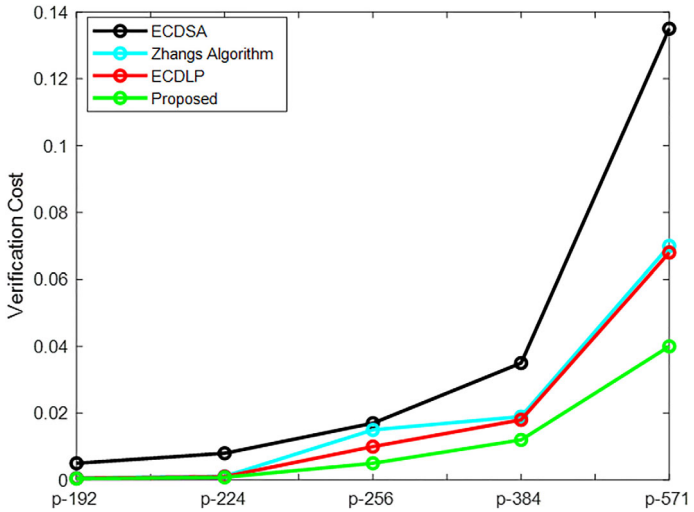

FIGURE 13 Signature verification cost.

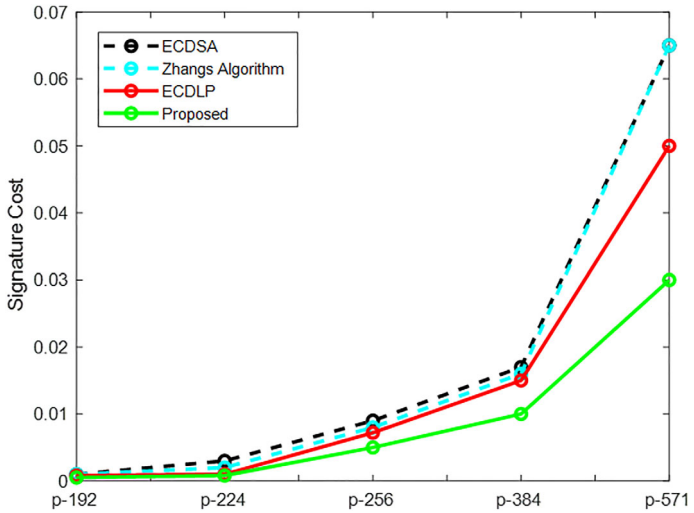

FIGURE 14 Signature generation cost.

reduced to ensure an improved performance rate. Here, the generated blocks and a varying number of IoT users have been considered for analysis. The results show that the latency of the proposed model is efficiently reduced to 0.2 s with the proper digital key generation and block construction operations. Moreover, the verification cost is also assessed concerning the varying packet sizes and several transactions. Here, the verification cost can be increased with the linear increase of the number of transactions, as shown in Figure 19. Then, the throughput is validated for the proposed methodology concerning various transactions, as depicted in Figure 20. The increased throughput rate assures reliable data

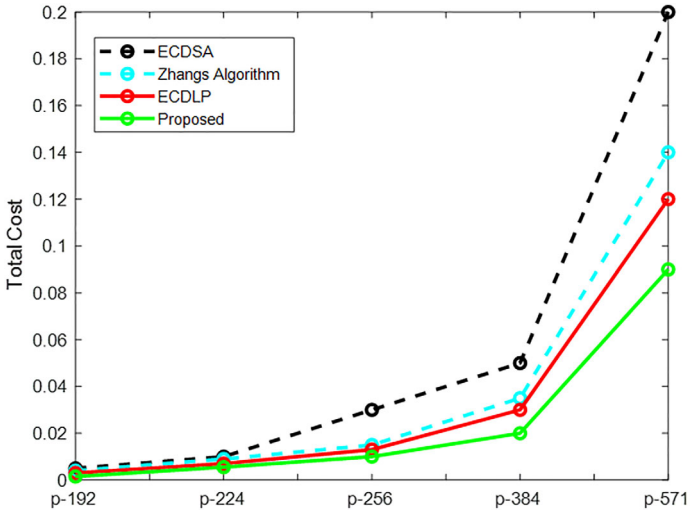

FIGURE 15 Total cost analysis.

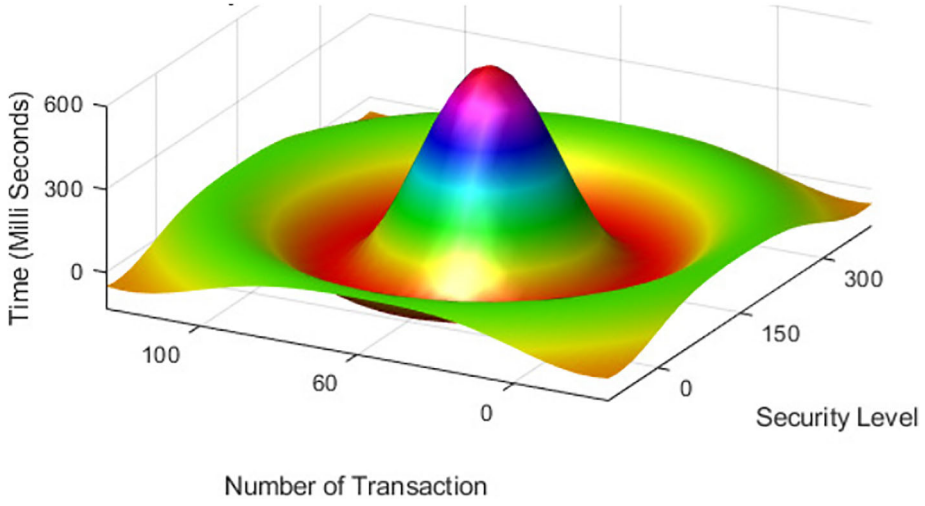

FIGURE 16 Time and level of security.

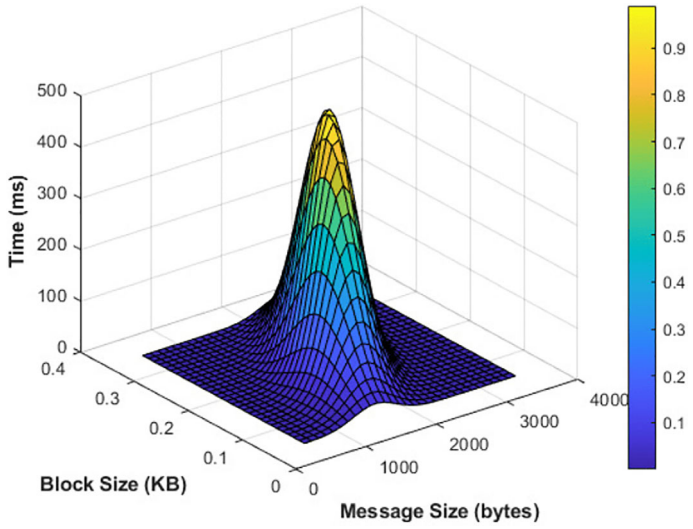

FIGURE 17 Time concerning varying block size.

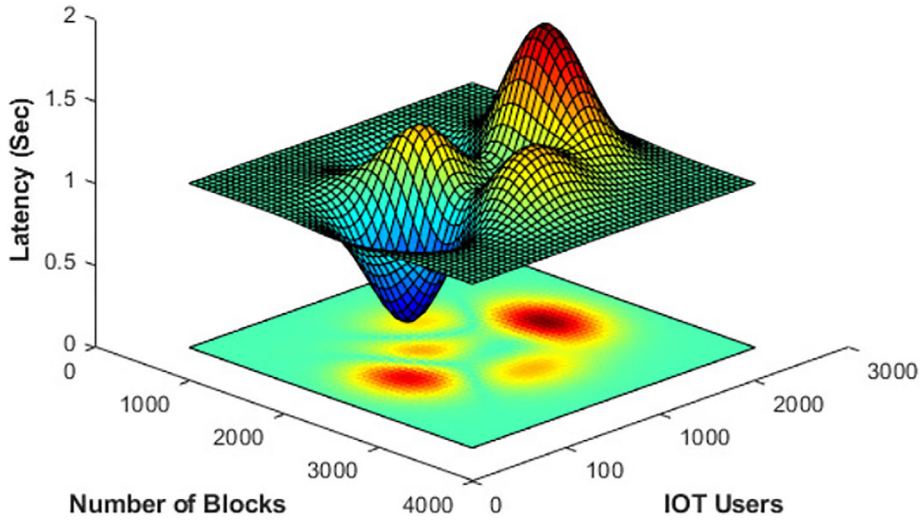

FIGURE 18 Latency analysis.

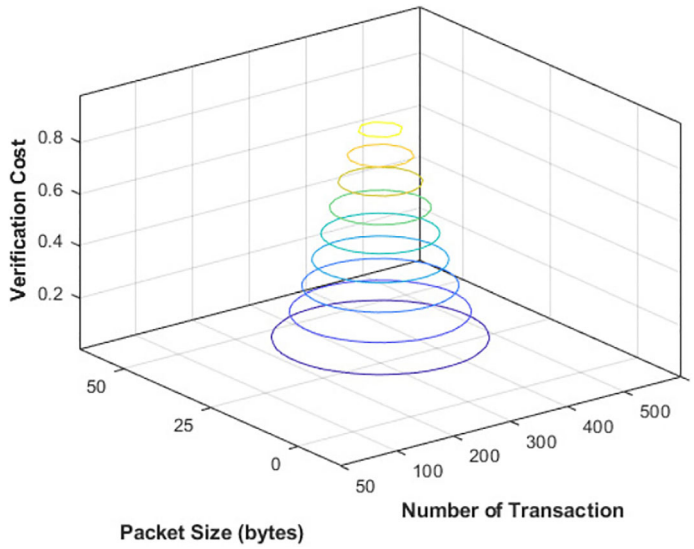

FIGURE 19 Verification cost analysis.

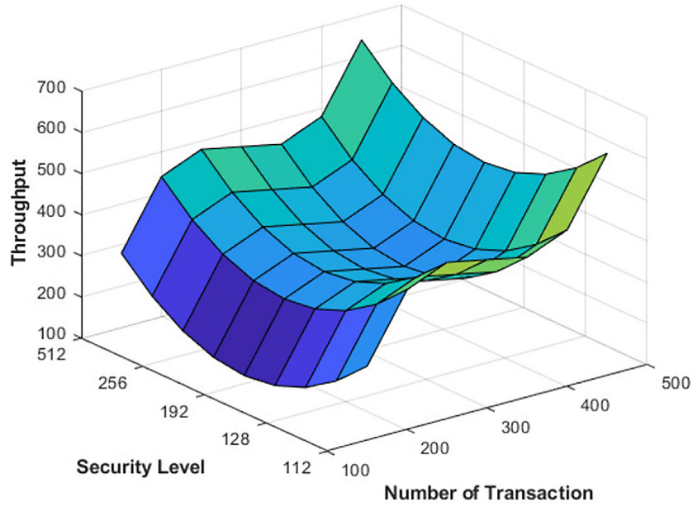

FIGURE 20 Throughput analysis.

TABLE 6 Performance study based on time.

Key length (bits)	Key generation time (ms)	Encryption time (ms)	Decryption time (ms)
32	100	15	20
64	150	20	40
128	1500	90	110
256	1800	150	125

TABLE 7 Security parameters for decentralized identifiable distributed ledger technology-blockchain.

Parameter	Description
Privacy	Very high
Security	Very high
Scalability	High
Authenticity	Yes
Confidentiality	Very high
Accuracy	Very high
Reliability	High
Exactness	High
Run time	Low

transactions in IoT systems. Due to the increased level of security, the throughput rate can be highly increased concerning a varying number of transactions.

Table 6 compares the amount of time in terms key generation time, encryption, and decryption time consumed by the proposed DIDLT-BC. Here, the time is analysed with respect to the key length (bits), and the findings indicate that the DIDLT-BC model consumes less amount for the entire security operations.

Table 7 discusses some of the security parameters that are effectively satisfied by the proposed DIDLT-BC methodology.

5 | CONCLUSION

This study developed a novel DIDLT-BC architecture to strengthen cloud-IoT system security against attackers. This work's primary contribution is creating a clever, effective blockchain security model with lower time and computational expenses. The modules for creating digital signatures, transaction initialization, key generation, transaction authentication, block construction using DIDLT, and validation are also included. In this instance, the signature used to initiate the data transaction was created using the Rabin digital signature technique. Initially, the hash function, elliptic curve, and integer field generated the users' private and public keys. Subsequently, the transaction originators can choose the public key set associated with the attribute values. Additionally, the primary purpose of the transaction originators' signatures is to prevent double-spending attacks in the distributed ledger system. The DIDLT model is used to generate the block header, hash code, timestamp, nonce message, and transaction list, which are used during block formation. The transaction signature can then be verified by any member who has the public key for the Rabin signature using the block verification process. Ultimately, the legality of a new block is verified as either valid or invalid based on the block formation process. If it is lawful, it can be added to the blockchain, and in order for other nodes in the network to receive the incoming data, they must synchronize with the new blocks. Furthermore, to provide solutions to operate under numerous unreliable nodes with various hash values, the BCA-based optimization methodology is employed. Several assessment metrics are used in performance analysis to verify and contrast the outcomes of the suggested DIDLT-BC model with those of the current models. The comparison analysis shows that the proposed mechanism performs better than the other methods regarding higher security, lower latency, low cost, and high throughput. The key advantages of the suggested methodology include authentication-based control, faster processing, safer data transfers, and less complexity. In future, the proposed work can be further enhanced by adopting the deep learning integrated blockchain methodology for healthcare IoT systems. Also, an access controlling model with activity protocol can be developed to protect healthcare data.

ACKNOWLEDGEMENTS

The authors of this study extend their appreciation to the Researchers Supporting Project number (RSPD2024R1034), King Saud University, Riyadh, Saudi Arabia.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

REFERENCES

Akhtar, M. M., Rizvi, D. R., Ahad, M. A., Kanhere, S. S., Amjad, M., & Coviello, G. (2021). Efficient data communication using distributed ledger technology and iota-enabled internet of things for a future machine-to-machine economy. *Sensors*, *21*, 4354.

Altun, C., & Tavli, B. (2019). Social internet of digital twins via distributed ledger technologies: Application of predictive maintenance. In *In 2019 27th telecommunications forum (TELFOR)* (pp. 1–4). IEEE.

Aluvalu, R., Kumaran, V. N. S., Thirumalaisamy, M., Basheer, S., Ali Aldhahri, E., & Selvarajan, S. (2023). Efficient data transmission on wireless communication through a privacy-enhanced blockchain process. *PeerJ Computer Science*, *9*, e1308. https://doi.org/10.7717/peerj-cs.1308

Aluvalu, R., Uma Maheswari, V., Chennam, K. K., & Shitharth, S. (2021). Data security in cloud computing using Abe-based access control. In *Architectural wireless networks solutions and security issues, ed: Springer* (pp. 47–61). Springer.

Balaji, B. S., Raja, P. V., Nayyar, A., Sanjeevikumar, P., & Pandiyan, S. (2020). Enhancement of security and handling the inconspicuousness in IoT using a simple size extensible blockchain. *Energies*, *13*, 1795.

Brotsis, S., Kolokotronis, N., Limniotis, K., Shiaeles, S., Kavallieros, D., Bellini, E., & Pavué, C. (2019). Blockchain solutions for forensic evidence preservation in IoT environments. *IEEE Conference on Network Softwarization (NetSoft), 2019*, 110–114.

Cullen, A., Ferraro, P., Sanders, W., Vigneri, L., & Shorten, R. (2021). Access control for distributed ledgers in the internet of things: A networking approach. *IEEE Internet of Things Journal*, *9*(3), 2277–2292.

Erdem, A., Yildirim, S. Ö., & Angin, P. (2019). Blockchain for ensuring security, privacy, and trust in IoT environments: The state of the art. *Security, Privacy and Trust in the IoT Environment*, 97–122. https://doi.org/10.1007/978-3-030-18075-1_6

Fan, Y., Zhao, G., Lei, X., Liang, W., Li, K.-C., Choo, K.-K. R., & Zhu, C. (2021). SBBS: A secure blockchain-based scheme for IoT data credibility in fog environment. *IEEE Internet of Things Journal*, *8*, 9268–9277.

Issa, W., Moustafa, N., Turnbull, B., Sohrabi, N., & Tari, Z. (2023). Blockchain-based federated learning for securing internet of things: A comprehensive survey. *ACM Computing Surveys*, *55*, 1–43.

Kalid, A., Ashfaq, N., Ashiq, W., Qureshi, M. A., & Arif, M. (2023). Trust Management in Smart Cities Using Blockchain Technology. In *Artificial Intelligence & Blockchain in cyber physical systems* (pp. 218–246). CRC Press.

Kamran, M., Khan, H. U., Nisar, W., Farooq, M., & Rehman, S.-U. (2020). Blockchain and internet of things: A bibliometric study. *Computers & Electrical Engineering*, *81*, 106525.

Khan, A. A., Bourouis, S., Kamruzzaman, M., Hadjouni, M., Shaikh, Z. A., Laghari, A. A., Elmannai, H., & Dhahbi, S. (2023). Data security in healthcare industrial internet of things with blockchain. *IEEE Sensors Journal*, *23*, 25144–25151.

Koshy, P., Babu, S., & Manoj, B. (2020). Sliding window blockchain architecture for internet of things. *IEEE Internet of Things Journal*, *7*, 3338–3348.

Kouzinopoulos, C. S., Spathoulas, G., Giannoutakis, K. M., Votis, K., Pandey, P., Tzovaras, D., et al. (2018). Using blockchains to strengthen the security of internet of things. In *International ISCIS Security Workshop* (pp. 90–100). Springer.

Laghari, A. A., Khan, A. A., Alkanhel, R., Elmannai, H., & Bourouis, S. (2023). Lightweight-biov: Blockchain distributed ledger technology (bdlt) for internet of vehicles (iovs). *Electronics*, *12*, 677.

Li, C., Tian, Y., Chen, X., & Li, J. (2021). An efficient anti-quantum lattice-based blind signature for blockchain-enabled systems. *Information Sciences*, *546*, 253–264.

Lim, J.-M., Kim, Y., & Yoo, C. (2018). Chain veri: Blockchain-based firmware verification system for IoT environment. In *2018 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)* (pp. 1050–1056). IEEE.

Liu, S.-G., Chen, W.-Q., & Liu, J.-L. (2021). An efficient double parameter elliptic curve digital signature algorithm for blockchain. *IEEE Access*, *9*, 77058–77066.

Mahajan, H., & Reddy, K. (2023). Secure gene profile data processing using lightweight cryptography and blockchain. *Cluster Computing*, 1–19. doi:10.1007/s10586-023-04123-6

Manoharan, H., Manoharan, A., Selvarajan, S., & Venkatachalam, K. (2023). Implementation of internet of things with blockchain using machine learning algorithm: Enhancement of security with blockchain. In T. Najar, et al. (Eds.), *Handbook of research on blockchain technology and the digitalization of the supply chain* (pp. 399–430). IGI Global. https://doi.org/10.4018/978-1-6684-7455-6.ch019

Mao, X., Li, C., Zhang, Y., Zhang, G., Li, J., Shah, M., & Xing, C. (2023). *HuaBaseChain: An extensible blockchain with high performance*. IEEE Internet of Things Journal.

Mazumdar, S., & Ruj, S. (2019). Design of anonymous endorsement system in hyperledger fabric. *IEEE Transactions on Emerging Topics in Computing*, *9*, 1780–1791.

Moin, S., Karim, A., Safdar, Z., Safdar, K., Ahmed, E., & Imran, M. (2019). Securing IoTs in distributed blockchain: Analysis, requirements and open issues. *Future Generation Computer Systems*, *100*, 325–343.

Nakanishi, R., Zhang, Y., Sasabe, M., & Kasahara, S. (2020). IOTA-based access control framework for the internet of things. In *2020 2nd conference on Blockchain Research & Applications for innovative networks and services (BRAINS)* (pp. 87–95). IEEE.

Padmaja, M., Shitharth, S., Prasuna, K., Chaturvedi, A., Kshirsagar, P. R., & Vani, A. (2021). Grow of artificial intelligence to challenge security in IoT application. *Wireless Personal Communications*, *127*, 1–17.

Rabie, O. B. J., Selvarajan, S., Hasanin, T., Mohammed, G. B., Alshareef, A. M., & Uddin, M. (2023). A full privacy-preserving distributed batch-based certificate-less aggregate signature authentication scheme for healthcare wearable wireless medical sensor networks (HWMSNs). *International Journal of Information Security*. https://doi.org/10.1007/s10207-023-00748-1

Rahman, A., Islam, M. J., Band, S. S., Muhammad, G., Hasan, K., & Tiwari, P. (2023). Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT. *Digital Communications and Networks*, *9*, 411–421.

Rahman, A., Islam, M. J., Rahman, Z., Reza, M. M., Anwar, A., Mahmud, M. P., Nasir, M. K., & Noor, R. M. (2020). Distb-condo: Distributed blockchain-based iot-sdn model for smart condominium. *IEEE Access*, *8*, 209594–209609.

Rakovic, V., Karamachoski, J., Atanasovski, V., & Gavrilovska, L. (2019). Blockchain paradigm and internet of things. *Wireless Personal Communications*, *106*, 219–235.

Ryu, J. H., Sharma, P. K., Jo, J. H., & Park, J. H. (2019). A blockchain-based decentralized efficient investigation framework for IoT digital forensics. *The Journal of Supercomputing*, *75*, 4372–4387.

Selvarajan, S., Manoharan, H., Khadidos, A. O., Shankar, A., Mekala, M. S., & Khadidos, A. O. (2023). RLIS: Resource limited improved security beyond fifth generation networks using deep learning algorithms. *IEEE Open Journal of the Communications Society*, *4*, 2383–2396. https://doi.org/10.1109/OJCOMS.2023.3318860

Selvarajan, S., Manoharan, H., Iwendi, C., Al-Shehari, T., Al-Razgan, M., & Alfakih, T. (2023). SCBC: Smart city monitoring with blockchain using internet of things for and neuro fuzzy procedures. *Mathematical Biosciences and Engineering*, *20*(12), 20828–20851. https://doi.org/10.3934/mbe.2023922

Selvarajan, S., & Mouratidis, H. (2023). A quantum trust and consultative transaction-based blockchain cybersecurity model for healthcare systems. *Scientific Reports*, *13*(1), 7107. https://doi.org/10.1038/s41598-023-34354-x

Selvarajan, S., Srivastava, G., Khadidos, A. O., Khadidos, A. O., Baza, M., Alsheri, A., & Lin, J. C.-W. (2023). An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems. *Journal of Cloud Computing*, *12*, 12–38.

Shahid, F., Khan, A., & Jeon, G. (2020). Post-quantum distributed ledger for internet of things. *Computers & Electrical Engineering*, *83*, 106581.

Shitharth, S., Alshareef, A. M., Khadidos, A. O., Alyoubi, K. H., Khadidos, A. O., & Uddin, M. (2023). A conjugate self-organizing migration (CSOM) and reconciliate multi-agent Markov learning (RMML) based cyborg intelligence mechanism for smart city security. *Scientific Reports*, *13*, 15681. https://doi.org/10.1038/s41598-023-42257-0

Selvarajan, S., Manoharan, H., Shankar, A., Alsowail, R. A., Pandiaraj, S., Edalatpanah, S. A., & Viriyasitavat, W. (2023). Federated learning optimization: A computational blockchain process with offloading analysis to enhance security. *Egyptian Informatics Journal*, *24*(4), 100406. https://doi.org/10.1016/j.eij.2023.100406

Sisi, Z., & Souri, A. (2021). Blockchain technology for energy-aware mobile crowd sensing approaches in internet of things. *Transactions on Emerging Telecommunications Technologies*, e4217. https://doi.org/10.1002/ett.4217

Sivaganesan, D. (2019). Block chain enabled internet of things. *Journal of Information Technology*, *1*, 1–8.

Son, M., & Kim, H. (2019). Blockchain-based secure firmware management system in IoT environment. In *2019 21st International Conference on Advanced Communication Technology (ICACT)* (pp. 142–146). IEEE.

Sowmiya, B., Poovammal, E., Ramana, K., Singh, S., & Yoon, B. (2021). Linear elliptical curve digital signature (LECDS) with blockchain approach for enhanced security on cloud server. *IEEE Access*, *9*, 138245–138253.

Thiruppathy Kesavan, V., Murugavalli, S., Premkumar, M., & Selvarajan, S. (2023). Adaptive neuro-fuzzy inference system and particle swarm optimization: A modern paradigm for securing VANETs. *IET Communications*, 1–18. https://doi.org/10.1049/cmu2.12692

Uddin, M., Selvarajan, S., Obaidat, M., Arfeen, S. U., Khadidos, A. O., Khadidos, A. O., & Abdelhaq, M. (2023). From hype to reality: Unveiling the promises, challenges and opportunities of blockchain in supply chain systems. *Sustainability*, *15*(16), 12193. https://doi.org/10.3390/su151612193

Velmurugadass, P., Dhanasekaran, S., Anand, S. S., & Vasudevan, V. (2021). Enhancing blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm. *Materials Today: Proceedings*, *37*, 2653–2659.

Vilas-Boas, J. L., Rodrigues, J. J., & Alberti, A. M. (2023). Convergence of distributed ledger technologies with digital twins, IoT, and AI for fresh food logistics: Challenges and opportunities. *Journal of Industrial Information Integration*, *31*, 100393.

Viriyasitavat, W., Da Xu, L., Bi, Z., & Pungpapong, V. (2019). Blockchain and internet of things for modern business process in digital economy—The state of the art. *IEEE Transactions on Computational Social Systems*, *6*, 1420–1432.

Xu, Y., Wang, G., Yang, J., Ren, J., Zhang, Y., & Zhang, C. (2018). Towards secure network computing services for lightweight clients using blockchain. *Wireless Communications and Mobile Computing*, *2018*, 1–12.

Yao, H., Mai, T., Wang, J., Ji, Z., Jiang, C., & Qian, Y. (2019). Resource trading in blockchain-based industrial internet of things. *IEEE Transactions on Industrial Informatics*, *15*, 3602–3609.

Zhang, P., Wang, L., Wang, W., Fu, K., & Wang, J. (2021). A blockchain system based on quantum-resistant digital signature. *Security and Communication Networks*, *Vol.*, *2021*, 1–13.

Zhang, W., Wu, Z., Han, G., Feng, Y., & Shu, L. (2020). Ldc: A lightweight dada consensus algorithm based on the blockchain for the industrial internet of things for smart city applications. *Future Generation Computer Systems*, *108*, 574–582.

Zhao, S., Li, S., & Yao, Y. (2019). Blockchain enabled industrial internet of things technology. *IEEE Transactions on Computational Social Systems*, *6*, 1442–1453.

Zhaofeng, M., Jialin, M., Jihui, W., & Zhiguang, S. (2020). Blockchain-based decentralized authentication modeling scheme in edge and IoT environment. *IEEE Internet of Things Journal*, *8*, 2116–2123.

Zhu, Q., Loke, S. W., Trujillo-Rasua, R., Jiang, F., & Xiang, Y. (2019). Applications of distributed ledger technologies to the internet of things: A survey. *ACM Computing Surveys (CSUR)*, *52*, 1–34.

AUTHOR BIOGRAPHIES

Dr Selvarajan Shitharth completed his PhD in the Department of Computers Science & Engineering, Anna University. He completed his Post-doc at The University of Essex, Colchester, UK. He has worked in various institutions with a teaching experience of seven years. Now, he is

working as a lecturer in cyber security at Leeds Beckett University, Leeds, UK. He has published in more than 85 International Journals and 20 International & National conferences. He has even published four patents in IPR. He is also an active member of IEEE Computer Society and five more professional bodies. He is also a member of the International Block chain organization. He is a certified hyperledger expert and certified Block chain developer. His current research interests include Cyber Security, Block chain, Critical Infrastructure & Systems, Network Security & Ethical Hacking. He is an active researcher, reviewer and editor for many international journals.

Dr Achyut Shankar is currently working as an Postdoc Research Fellow at University of Warwick, United Kingdom and recently appointed as visiting Associate Professor at University of Johannesburg, South Africa. He obtained his PhD in Computer Science and Engineering majoring in wireless sensor network from VIT University, Vellore, India. He was at Birkbeck University, London from Jan 2022 to May 2022 for his research work. He has published more than 90 research papers in reputed international conferences & journals in which 65 papers are in SCIE journals. He is a member of ACM and has received research award for excellence in research for the year 2016 and 2017. He is serving as reviewer of IEEE Transactions on Intelligent Transportation Systems, IEEE Sensors Journal, IEEE Internet of Things Journal, ACM Transactions on Asian and Low-Resource Language Information Processing and other prestigious conferences. His areas of interest include Wireless sensor network, Machine Learning, Internet of Thing, Block-chain and Cloud computing.

Mueen Uddin received his Ph.D. degree from the Universiti Teknologi Malaysia (UTM), in 2013. He is currently working as an Associate Professor of Cybersecurity and Data Sciences at the University of Doha for Science and Technology Qatar. He has published over 130 international journals and conference papers in highly reputed journals with a cumulative impact factor of over 300. His research interests include Block chain, Cybersecurity, IoT, Network Security and Cloud Computing.

Abdullah Saleh Alqahtani is currently working as an Associate Professor in Computer Science at Common First Year Deanship, Department of Self- Development Skills, King Saud University, Riyadh, Saudi Arabia. He received his Ph.D. and Master's degree from School of Computer Science, Engineering and Mathematics under the Faculty of Science and Engineering at Flinders University, Adelaide, Australia. His area of specializations includes Data Analytics on E-commerce, E-Business and Data Optimization by Structural Equation Modeling. His current area of research interests includes Optimization, Computational Algorithms, Data science, Deep Learning and Artificial intelligence.

Taher Al-Shehari received the B.S. degree in computer science from King Khalid University, Saudi Arabia, in 2007, and the M.S. degree in computer science from the King Fahd University of Petroleum and Minerals (KFUPM), in 2014. From 2011 to 2014, he was a Research Assistant with the King Fahd University of Petroleum and Minerals. Since 2015, he has been a Senior Lecturer and a Researcher with King Saud University. He is the author of several articles that are published in prestige journals. His research interests include information security and privacy, insider threat detection and prevention systems, machine learning models, and data analysis. His awards and honors include, the Honor Award from King Khalid University's Rector; and the Best Designed Curriculum Award from CFY's Dean, KSU.

Wattana Viriyasitavat is an Associate Professor of Information Technology at Chulalongkorn University, Bangkok, Thailand. He received the D.Phil. degree (Ph.D.) in computer science from the University of Oxford, Oxford, U.K., in 2013. He is an IEEE Senior member (2019). Presently, he is a full-time lecturer and researcher with the Business Information Technology Division, Department of Statistics, Faculty of Commerce and Accountancy, Chulalongkorn University. He is a co-Founder and Chief Technology officer of Prime Capture, a startup company and has served as a consultant in a few leading organizations namely Tourism Authority of Thailand, Bank for Agriculture and Agricultural Cooperatives, and Metropolitan Electricity Authority. He is also certified by ISO 15540 as a professional assessor He has served as an editorial advisory member for Journal of Industrial Information Integration. His received annual research awards from National Research Council of Thailand (2007), and the 2016 Thailand Frontier Researcher Awards (Thomson Reuters).

How to cite this article: Selvarajan, S., Shankar, A., Uddin, M., Alqahtani, A. S., Al-Shehari, T., & Viriyasitavat, W. (2024). A smart decentralized identifiable distributed ledger technology-based blockchain (DIDLT-BC) model for cloud-IoT security. *Expert Systems*, e13544. https://doi.org/10.1111/exsy.13544