


Article

A New Blockchain-Based Authentication Framework for Secure IoT Networks

Ahmad K. Al Hwaitat ¹, Mohammed Amin Almaiah ^{1,2,*} , Aitizaz Ali ³, Shaha Al-Otaibi ^{4,*}, Rima Shishakly ⁵, Abdalwali Lutfi ^{6,7} and Mahmaod Alrawad ⁶

¹ King Abdullah the II IT School, Department of Computer Science, The University of Jordan, Amman 11942, Jordan

² Fellowship Researcher, INTI International University, Nilai 71800, Malaysia

³ School of IT, UNITAR International University, Petaling Jaya 47301, Malaysia; aitizazz.ali@monash.edu

⁴ Department of Information Systems, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia

⁵ Management Department, College of Business Administration, Ajman University, Ajman 346, United Arab Emirates; r.shishaky@ajman.ac.ae

⁶ College of Business Administration, King Faisal University, Al-Ahsa 31982, Saudi Arabia; aalkhassawneh@kfu.edu.sa (A.L.)

⁷ Applied Science Research Center, Applied Science Private University, Amman 11931, Jordan

* Correspondence: m_almaiah@asu.edu.jo (M.A.A.); stalotaibi@pnu.edu.sa (S.A.-O.)

Abstract: Most current research on decentralized IoT applications focuses on a specific vulnerability. However, for IoT applications, only a limited number of techniques are dedicated to handling privacy and trust concerns. To address that, blockchain-based solutions that improve the quality of IoT networks are becoming increasingly used. In the context of IoT security, a blockchain-based authentication framework could be used to store and verify the identities of devices in a decentralized manner, allowing them to communicate with each other and with external systems in a secure and trust-less manner. The main issues in the existing blockchain-based IoT system are the complexity and storage overhead. To solve these research issues, we have proposed a unique approach for a massive IoT system based on a permissions-based blockchain that provides data storage optimization and a lightweight authentication mechanism to the users. The proposed method can provide a solution to most of the applications which rely on blockchain technology, especially in assisting with scalability and optimized storage. Additionally, for the first time, we have integrated homomorphic encryption to encrypt the IoT data at the user's end and upload it to the cloud. The proposed method is compared with other benchmark frameworks based on extensive simulation results. Our research contributes by designing a novel IoT approach based on a trust-aware security approach that increases security and privacy while connecting outstanding IoT services.

Keywords: security; privacy; blockchain; smart contracts; IoT; encryption; transaction



Citation: Al Hwaitat, A.K.; Almaiah, M.A.; Ali, A.; Al-Otaibi, S.; Shishakly, R.; Lutfi, A.; Alrawad, M. A New Blockchain-Based Authentication Framework for Secure IoT Networks. *Electronics* **2023**, *12*, 3618. <https://doi.org/10.3390/electronics12173618>

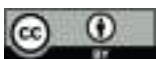
Academic Editors: Satyabrata Aich, Kamalakanta Muduli and Sushanta Tripathy

Received: 5 July 2023

Revised: 6 August 2023

Accepted: 7 August 2023

Published: 27 August 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The proliferation of industrial IoT applications and networking services has facilitated a tremendous increase in the number of connected devices. These application devices can capture real-time industrial data with a dedicated sensor unit [1]. Industrial advancement and technological guidance are behind this shift in how systems interact with physical and logical things. A centralized architecture is used to communicate real-time industrial data and evaluate the critical components of IoT, including identity management [2]. A single failure point is feasible due to this common technique [3]. A significant issue with the Internet of Things (IoT) is the difficulty in maintaining and managing many connected devices [4]. A system of networks can talk interactively through adaptive self-configuration. IoT applications can be commercialized over the 6G network. A fundamental component

of the IoT, the wireless sensor network (WSN) gathers and transmits physical data using various heterogeneous models [5].

Data security is a major concern of IoT systems because they are built by connecting many IoT devices [6]. Data generated by these devices are stored in the cloud and transmitted across various networks. A cyber-attack on a smart healthcare system can substantially impact the system's ability to produce and supply electricity. In addition to financial and other types of damage, cyber-attacks on smart healthcare can cause operational failures, power outages, the theft of critical data, and complete security breaches [7]. Cyber experts face difficulties keeping tabs on everything that passes via a smart grid and recognizing potential threats and attacks. Even though machine learning has become an essential part of cybersecurity, the problem is that this field requires distinct approaches and theoretical viewpoints to handle the enormous volume of data generated and transported across numerous networks in a smart grid [8]. The attacks and threats that could be launched against this proof-of-concept environment are being determined using threat modeling. Several potential threats have been tested, including detection, tampering, repudiation, information leakage, denial of service (DoS), and extended privilege (EoP). Each of the risks and the security elements associated with them are addressed using STRIDE. STRIDE is a typical threat modeling technique for finding and classifying attack vectors [9]. Using the well-known industrial framework MITRE ATTCK, researchers can detect threats disguised as tactics, techniques, and procedures (TTP) [10].

Based on the above, blockchain technology could be one of the main solutions for IoT security issues [11]. A blockchain provides a decentralized system using a consensus mechanism and smart contracts [12]. Smart contracts are the protocols that trigger the blockchain to act according to a particular activity or situation [13]. Blockchains can be categorized into three classes: private, public, and hybrid public blockchain technology. The main feature of a blockchain is to provide security and only keep records and transactions within a single organization. A public blockchain provides access to the public using a public API. Moreover, such a model interacts with external networks such as gateway networks or cloud outsourcing. A hybrid blockchain is also called a consortium blockchain, which provides features of both a private and public blockchain. This research used a hybrid blockchain to interact with an IoT system. The proposed model receives data from IoT sensors, verifies them, and encrypts them using homomorphic encryption. Homomorphic encryption is introduced in this approach for the first time. The primary function of homomorphic encryption is to encrypt a user's data at the user layer and outsource them to the cloud. This approach provides the facility to perform any statistical and machine learning operation on encrypted data. This IoT-based network consists of thousands of tiny sensors attached to the human body to remotely detect conditions such as heart rate, blood pressure, temperature, and sugar level. The data collected from these thousand sensors are massive data that need training, testing, validation, and an authentication system. IoT management systems exist, but there are also security issues due to inefficient authentication, which is discussed more in the literature. The proposed model trains the IoT-based healthcare data using a hybrid deep learning approach and predicts the patient's condition without needing a clinician or physician. The proposed framework provides privacy preservation, security, and lightweight authentication.

The research presents the following contributions: (1) the design of a novel IoT approach based on a trust-aware security approach increases security and privacy while connecting outstanding IoT services; (2) the sensing units generate industrial data across a dedicated network to concentrate the application service structure; (3) the network architecture connects to a variety of trustworthy IoT devices to meet 6G-enabled IoT requirements, and the proposed algorithms are enhanced with individual data such as biometric, video, and speech data.

The paper is organized as follows: Section 2 explains the background of the proposed research and the preliminary work. Contributions to this research are explained in Section 3. The proposed methodology is explained in Section 4. The experimental setup and simula-

tion results are discussed in Section 5. The conclusion and future directions are given in Section 6.

2. Background and Related Studies

Blockchain technology can be used to build trust and monitor node activity in IoT networks. It is challenging to integrate a blockchain into IoT applications due to its high power consumption and job outsourcing [14]. Several blockchain-based Internet of Things (IoT) applications have recently been created to address these concerns. These blocks can be used to delete old transactions and blocks from the blockchain without jeopardizing security. Pan et al. [15] created an IoT resource management prototype using blockchain technology and smart contracts to securely record all IoT transactions [15]. Deploying smart contracts involves evaluating the source code, bytes of code, and execution histories. This is how we test our computer traffic analysis deployment scenario. Ali et al. [16] investigated blockchain technology and smart contract applications in cloud storage. Tam et al. utilize a pay-as-you-go car business model. This technology's strengths are traceability and tamper-proof characteristics. Ali et al. [17] created a blockchain-based publisher-subscriber model. They designed their solution to ensure data integrity in real-time IoT processing by balancing computational resources and workload. Liu et al. delegated computationally intensive POW mining tasks to nearby edge servers in blockchain-enabled mobile IoT systems [18]. Chen et al. conducted additional research. Securing biometric data for patient authentication is a common issue. In particular, finger vein biometric data has been studied extensively. A strong verification mechanism with high levels of reliability, privacy, and security is required to better secure these data. Also, biometric data are difficult to replace, and any leakage of biometric data exposes users to serious threats, such as replay attacks employing stolen biometric data. This research offers a unique verification secure framework based on triplex blockchain-based particle swarm optimization (PSO)-advanced encryption standard (AES) approaches in medical systems for patient authentication. The discussion has three stages. First presented is a new hybrid model pattern based on RFID and finger vein biometrics to boost randomness. It proposes a new merge method that combines RFID and finger vein characteristics in a random pattern. Second, the suggested verification safe framework is based on the CIA standard for telemedicine authentication using AES encryption, blockchain technology, and PSO in steganography [19]. Finally, the proposed secure verification architecture was validated and evaluated [20]. The combination of WSN functional activities with 6G network topologies allows us to test a wide range of IoT application deployment models. Many IoT devices collect data using IPV6 across low-power wireless personal area networks and wearables (6LoWPAN) [21,22]. We were able to keep user data confidential with the help of AKA [23]. Companies that use public cloud services and large-scale data storage systems have long prioritized client data protection [24].

Some studies have used other approaches such as physical layer security (PLS) in order to ensure secure transmission via a signal and reduce the quality of the signal in the attacker device [25–30]. As compared with other security approaches, the PLS approach has several strong advantages, such as the PLS technique does not depend on keys in the encryption/decryption processes, which will help through minimizing the difficulty of the secret keys distribution and its management in an IoT environment [31–34]. In addition, the PLS approach uses simple signal processing algorithms, which need low overhead as compared to other encryption methods. Recognizing the value of reliable data in decision-making batch processing may be required when working with huge datasets in the cloud. Even so, comparing the two seems impossible [35]. To safeguard user passwords, Edward et al. [36] examined privacy laws and regulations. In real-time data communication with the Internet, dispersed mobility management rules and smart computer activities are separated. Unlike real-time systems, cryptographic algorithms establish a public/private key pair. The cloud server can read private cloud data by sharing a secret key [37]. Statista predicts there will be 50 billion connected IoT devices by 2030. As

a result, the market will increase rapidly in the future. Consistently protecting user privacy, blockchain-based trust might be used to provide seamless authentication (TAB-SAPP). Smart design architecture is presented for spreading device connectivity over physical networks. Zigbee, Z-Wave, and Bluetooth Low Energy (BLE) are the most widely used industrial automation standards. The blockchain's peer-to-peer nature allows IoT devices to connect to each other. Decentralized IoT devices and consensus methods generate and store data in encrypted chain-like blocks, while smart contracts modify data and control the system [38]. Blockchain-enabled IoT relies on a secure security paradigm (also known as IoT-EBT). This is possible because smart contracts retain and limit computing resources associated with a device's identification [39].

Different applications demand different levels of security, and resource scarcity plays a factor. Finding the best encryption technique for IoT medical data protection is essential [40–43]. Electronic sensors capture medical data from patients and safely transmit them to the healthcare system. To avoid unwanted access or needless interruptions, trust and data privacy must be ensured from the start sensors [44–46].

Thus, data encryption from the start sensors is required, but due to restrictions in CPU complexity, battery consumption, and transmission bandwidth, using standard crypto algorithms is impractical [47–50]. Research on realistic, lightweight encryption techniques for IoT medical systems is ongoing. This study compares eight cryptographic algorithms in terms of memory usage and speed. The study determines the best candidate algorithm for the proposed health care system, balancing the ideal requirement and future dangers [51–54]. Both parties must be authenticated to use these services safely [55–58]. The server should require authentication to protect records from unauthorized users and ensure patient privacy (client side). Patient authentication is required to prevent server impersonation [59–62]. This proof of concept addresses emergency situations where a patient arrives unconscious at the hospital and needs to access information without providing an authorization key. This issue requires safe biometric identification technologies such as palm vein and iris [63–66]. In addition to providing high levels of security, usability, and dependability, biometric technology authentication has grown in popularity [67–72]. For example, the finger vein (FV) biometric is highly secure. Most modern authentication systems save biometric patterns in a database. Authentication extracts this data as biological biometrics. Secure biometric authentication with FV will be more resistant to security breaches and impersonation attempts. The human FV is a physiological biometric used to identify people by their blood veins' morphological characteristics. Individuals and offenders (in legal situations) are identified using this new technology, which is more accurate than other biometric systems. In order to secure FV biometrics, many researchers have used uni- or multi-biometrics, which include FV biometrics as part of the verification system. These approaches are applied in two steps as follows: To protect FV patterns, researchers are trying to extract trustworthy properties from FVs, which can be used to uniquely identify individuals. These exclusive properties from the FV junction sites and the angles between veins are used to build a unique key (biokey). This key is used to encrypt data patterns. The observation matrix extracts patterns and features, which are then encrypted with a random key [73]. Some researchers employed multi-biometrics to add to existing features. These traits have been used to identify people (FV, retina, and fingerprint). The main issues with the system the author devised in [74–76] were communication cost and computational cost.

2.1. Overview of Blockchain Structure

A blockchain is a decentralized, distributed ledger that is used to record transactions across a network of computers [77]. Each block in the chain contains a record of multiple transactions, and once a block is added to the chain, it cannot be altered [78]. This makes the blockchain a secure and transparent way to store data. As shown in Figure 1, the data structure of a blockchain is typically a linked list of blocks, with each block containing a set of transactions. The transactions are organized using a data structure called a Merkle tree, which facilitates efficient verification of the integrity of the transactions. The data model

for a blockchain is typically based on a distributed ledger model, in which the ledger is maintained and updated by a network of computers rather than a central authority. The ledger is structured as a chain of blocks, with each block containing a set of transactions and a cryptographic hash of the previous block. This structure facilitates the secure and transparent storage of data on the blockchain [79]. In a blockchain, the data are stored in a decentralized manner, with copies of the ledger being maintained by multiple nodes on the network [80]. This ensures that the data are secure and cannot be altered without the consensus of the network [81]. Each transaction on the blockchain is cryptographically signed, providing a secure and verifiable record of the transaction [82]. Overall, the data structure and data model of a blockchain are designed to provide a secure and transparent way to store and manage data in a decentralized manner.

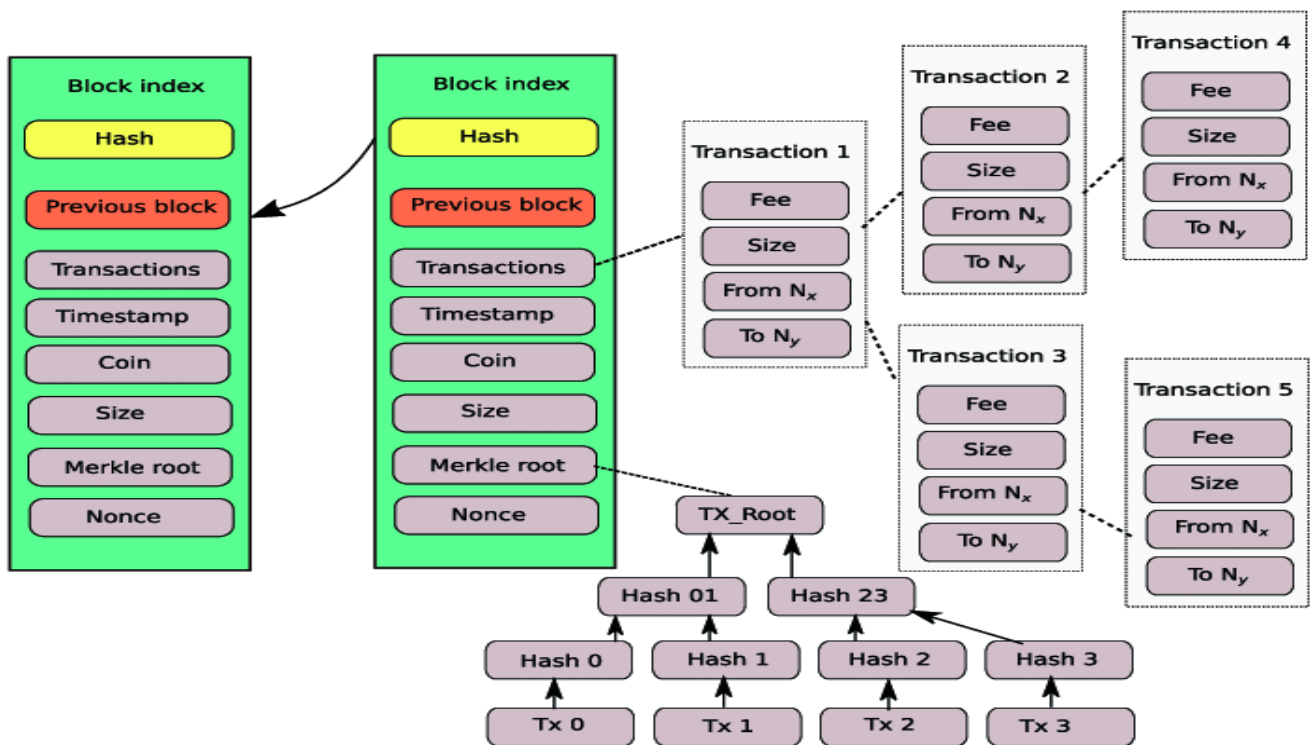


Figure 1. The blockchain data structure.

2.2. IoT Data Flow

IoT data refer to the vast amount of information generated by connected devices and sensors that comprise the Internet of Things. These devices can include anything from industrial machinery and consumer appliances to vehicles and home security systems. The data generated by these devices can include a wide variety of information, such as sensor readings, GPS coordinates, usage patterns, etc.

IoT data and blockchain technology can be combined through the use of smart contracts. A smart contract is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the transactions are stored on a blockchain network, making them transparent and secure. Smart contracts can be used to automate the process of collecting and storing IoT data on the blockchain, creating a tamper-proof record of the data.

As shown in Figure 2, one way to authenticate IoT data using blockchain technology is through the use of blockchain-based smart contracts to authenticate the data. In this model, the smart contract is programmed to verify the authenticity of the data before it is recorded on the blockchain [31]. This can help ensure that only authentic data are stored on the blockchain, increasing the reliability and trustworthiness of the data. In this study,

the use of smart contracts can help to provide a secure and verifiable way to authenticate IoT data using blockchain technology.

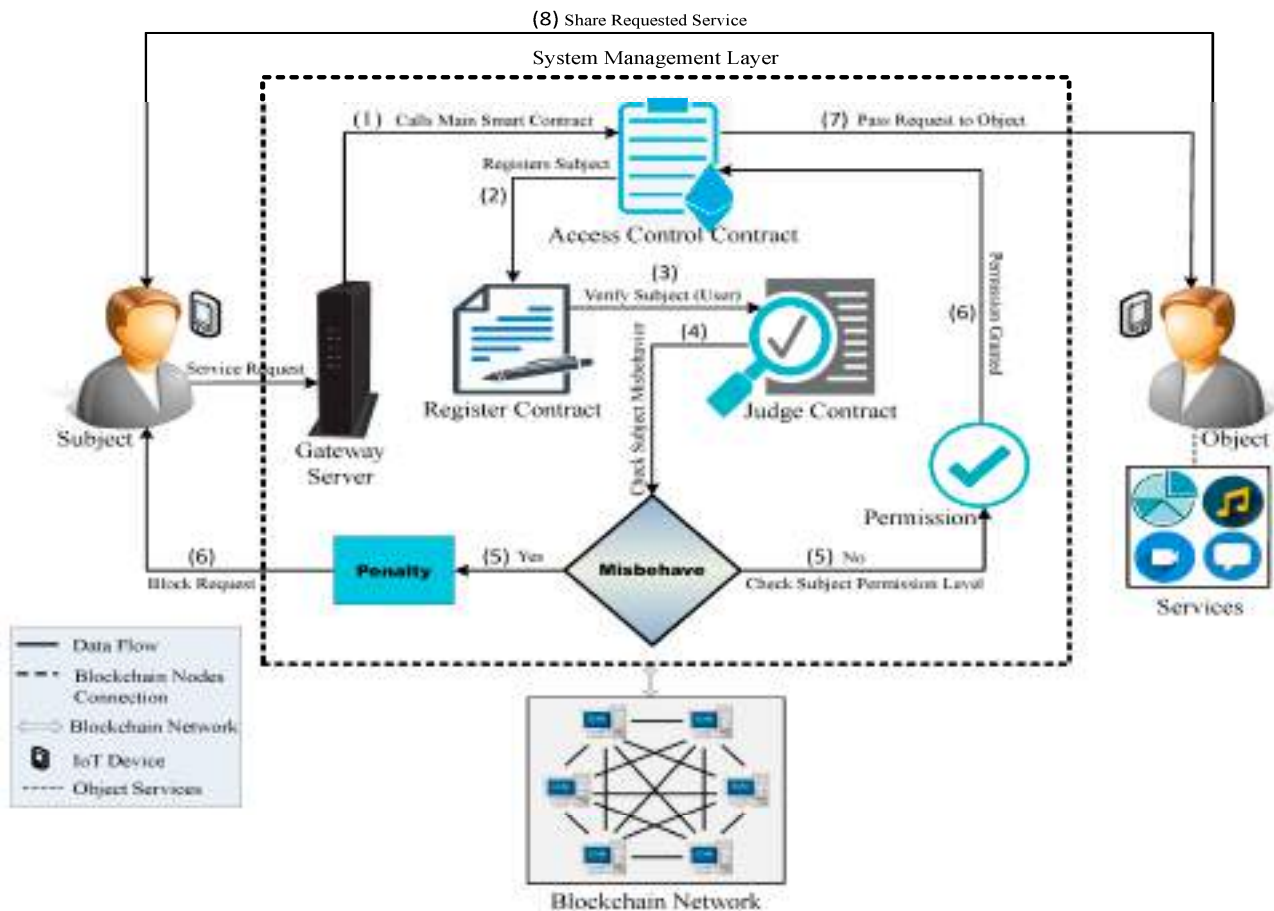


Figure 2. IoT using blockchain smart contracts.

3. Methodology

The proposed methodology consists of the steps that have been carried out during the experiments in order to obtain the system output. The subsections below represent the steps involved in the proposed methodology, and how the system works is explained through a schematic diagram as shown below. In step 1, the IoT data are collected from the sensors and sent to the cluster head. In step 2, the data transaction through the blockchain takes place. Data are verified and authenticated from IoT edge devices which are in large quantity. In the next step, data are encrypted using homomorphic encryption and then outsourced to the cloud. The integration of homomorphic encryption provides the facility that any kind of statistical and deep learning operation can be performed over encrypted data. Feature extraction is the next step in our proposed framework, in which features are extracted from the data such as heart rate, age, sex, weight, and height. Moreover, the proposed framework uses SVM to classify the users and the data based on the features and interaction with the system that took place. Finally, the output is verified and validated through a validation model.

3.1. Proposed Algorithms

In order to implement the proposed framework, we have proposed a novel algorithm in order to govern the proposed framework. The function of this algorithm is explained in detail step by step as follows: Algorithm 1 defines the working of updates, creating and revoking the policy. Moreover, the algorithm first creates the PHR on the request of a user, then it updates the existing PHR, and at the end, it revokes the PHR if the user

violates the access control policy. Algorithm 1 defines the attribute assigned to the patients and clinicians.

Algorithm 1 Algorithm for Create, Update and Revoke Records.

Input: ID and key requested from Nadmin

2: Output: Get access to PHL transactions

Initialization: PHL should be valid node. PHL can Read/Write/Grant/Revoke EHR records.

4: procedure Ptient

($P_i d$) while (True)

do

6: if ($P_i d B_N$) then

if ($PREC_I \text{ not } B_N$) then

8: Create_records ($P_i d, PREC_I, B_N$)

else

10: Update_records ($P_i d, PREC_I, B_N$)

Read_records ($PID, PREC_I, CID, L_i d, B_N$)

12: end if

else

14: Not_exist ($P_i d$)

end if

16: if Visit ($P_i d, C_i d, L_i d, B_N$) then MPID = Medrecord ($P_i d$)

18: if then ($MP_i d, PHL, B_N$)

Grant_records ($MP_i d, C_i d, L_i d, B_N$)

20: else

($C_i d, L_i d$) = NOTIFY (record does not exist)

22: end if

if ($P_i d C_i d, L_i d$ Treatment – completed ($P_i d$))

24: then

Revoke-records ($MP_i d, P_i d, C_i d, L_i d, B_N$)

26: else

($C_i d, L_i d$) = NOTIFY($P_i d$ revoke $MP_i d$)

28: Revoke-records ($MP_i d, P_i d, C_i d, L_i d, B_N$)

end if

30: else

Not Visit

32: end if

end **while**

34: end procedure

Algorithm 2 checks the attributes by assigning the master key, signature count, and bi-linear pair group. The user selects a random value from a group of bilinear pairs, such as G1 and G2. Furthermore, Algorithm 2 is used to define the method evaluation of the proposed model and the attribute associated with it. It evaluates the parameters and attributes designed to authenticate the user request to the system. The algorithm describes the design and use of homomorphic encryption. We have used homomorphic encryption within our proposed model. The main benefit of the proposed homomorphic encryption is to perform any operation over encrypted data without decryption.

Algorithm 3 defines the algorithm's working, which explains the working of cluster head selection. Based on the battery power, the proposed algorithm selects the cluster head from one of the sensors and receives the IoT data from the other nodes.

Algorithm 4 presents the step-by-step working of the algorithm used to encrypt EMR with homomorphic encryption (HE). Homomorphic encryption allows users or AI models to perform complex statistical or mathematical operations without decryption, as it can be achieved on plain text. HE allows the users to encrypt data at their side and outsource to the cloud, which leads to security and privacy preservation. Moreover, there are three types of homomorphic encryption: fully HE, partially HE, and hybrid HE. In this research,

we used fully homomorphic encryption due to the proposed approach requirements and integration with the IoMT devices that are more in number.

Algorithm 2 Algorithm for Attribute Assigning.

Initialization: Master Public Key public domain
 2: Select random Numbers
 Initialization: PHL should be valid node
 4: Compute $w = H(h, d, N)$
 Compute $\sigma = H(h, \sigma, r)$ (True) do
 6: Calculate Value $u = e(S, P)$ in G
 Compute $w = u.t$ in G
 8: Create_records (Pid, PREC_I, BN)
 Else
 10: Update_records (Pid, PREC_I, BN)
 Read_records (PID, PREC_I, CID, Lid, BN)
 12: end if
 Else
 14: Not_exist (Pid)
 End if
 16: if Visit (Pid, Cid, Lid, BN) then MPID = Medrecord (Pid)
 18: if then (MPid, PHL, BN)
 Grant_records (MPid, Cid, Lid, BN)
 20: else
 (Cid, Lid) = NOTIFY (Medical record does not exist)
 22: end if
 If $h_2 = H_2(W_0 \rightarrow W_n, N)$ Verification successful
 24: else
 Verification Fails
 26: end if else
 28: end if
 End procedure

Algorithm 3 Algorithm for selection of Cluster Head.

Input: ID and key requested from Network admin
Output: Get access to IoT transactions
Initialization: CH should be valid node. CH can Read/Write Permission allotted IOT records by the patients and write medical records of the patients.
 Procedure Clinician ($C_i d$)
 While (True)
 Do
 if ($C_i DB_N$) then If
 (Granted $MP_{i_d} C_{i_d}$) then
 Read_records ($C_{i_d}, PREC_{i_d}, MP_{i_d}, B_N$) Update_records ($C_{i_d}, PREC_{i_d}, MP_{i_d}, B_N$) else
 Write_records (C_{i_d}, MP_{i_d}, B_N)
 Read_records (C_{i_d}, L_{i_d}, B_N)
 end if
 else Not_exist(C_{i_d}) end if
 end **while**
 End procedure

3.2. System Model

An industrial automation authentication system that is both trustworthy and simple is the purpose of this section. Private keys can be tested for security using a multi-signature-compatible contract, ensuring that no one else has access. Industrial automation will create a pay-as-you-go intelligent approach to explore the computing processes of IoT gadgets. Figure 2 presents the application of IoT and its impact on the technology. IoT consists of

thousands and millions of tiny sensors, edge devices, computers, Wi-Fi, and RFID, and all these devices generate data. Data received from these devices are so massive that security breaches and data mismanagement can easily happen. A multi-signature-compatible contract examines all aspects of a transaction, from quality control to mechanical technique to decision-making. To make independent decisions, the intelligent model makes use of traffic patterns. An IoT device’s fundamental operational operations are analyzed by a smart contract to maximize overall system efficiency.

Algorithm 4 Homomorphic Encryption.

1. Initialize Public Key
 2. $T \rightarrow 0$, keywords W
 3. Select key KS for PRF
 4. Select keys KX, KI, KZ for PRF F_p
 5. Z^*p and parse DB as $(idi, Widi)_{di=1}$
 6. $t \leftarrow N$
 7. $Ke \leftarrow F(KS, w)$
 8. $id \in DB(w)$ do Counter $c \leftarrow 1$
 9. Compute $xid \leftarrow F_p(KI, id)$, $z \leftarrow F_p(KZ, w || c)$
 10. $y \leftarrow xidz - 1e \leftarrow Enc(Ke, id)$.
 11. $xtag \leftarrow gF_p(KX, w)xid$ and $XSet \leftarrow XSet \cup xtag$
 12. Append (y, e) to t and $c \leftarrow c + 1$
 13. $T[w] \leftarrow t$ ($TSet, KT$) $\leftarrow TSet.Setup(T)$
 14. let $EDB = (TSet, XSet)$
 15. return $EDB, K = (KS, KX, KI, KZ, KT)$
 16. If token $\leq (q(w), K) \rightarrow'$
 17. Client’s input is K and query $q(w = (w1, \dots, wn))$
 18. Compute $stag \rightarrow TSet.GetTag(KT, w1)$
 19. Repeat step 18
 20. Until $stag \rightarrow 0$
 19. Client sends $stag$ to the server
 20. $c = 1, 2, \dots$ until the server stops
 21. $i = 2, \dots, n$ to $en [c,i] \leftarrow gF_p(KZ, w1 || c)F_p(KX, wi)$ $xtoken [c] \leftarrow (xtoken, \dots, xto ken[c,n])$
 22. $Tokq \leftarrow (stag, xtoken)$
 23. return $T okq$
 24. Searching Technique
 25. $ERes \leftarrow t \rightarrow TSet(Retrieve)(TSet, stag)$
 26. Verification result: succeed
-

Table 1 shows how scientists use the TAB-SAPP notation. Figure 3 represent the application of cloud computing in various organizations. Cloud provides on-demand resource allocation anywhere, anytime, and any place. Moreover, three types of the cloud exist depending on the application of the cloud and usage, such as private, public and hybrid cloud [30,31].

Table 1. Simulation setup, configurations, and specifications.

Parameters	Details
Dataset size	100 number of blocks + PHR
Hardware Software Parameters	GPU-enabled system Ethereum, hyperledger fabric
Performance Metric	Block height, number of blocks, No. transactions, No. PHR, delay, signature creation
Number of simulations Number of rounds or transactions	Efficiency (average percentage of Gas, no. packets, no. dead nodes, no. alive nodes), security (the execution time of policies) and cost (execution time of blocks), Number of tests performed on single dataset: 5000

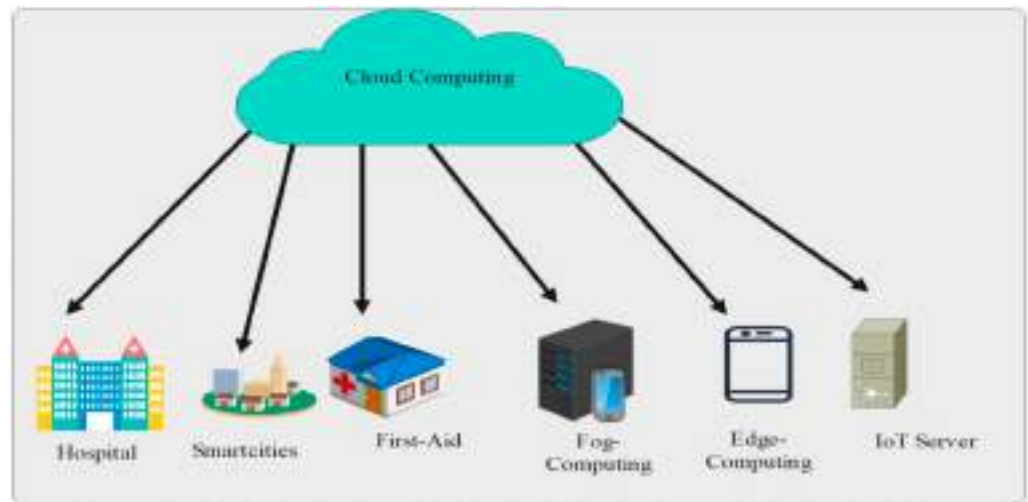


Figure 3. Application of cloud computing.

Communication components include the following: An external owner account can access a billfold contract. A reliable transaction can address the different IoT devices scattered by automation. Automation and control experts are needed to distribute and manage large IoT devices.

Figure 4 presents a schematic of the proposed smart contracts for authentication and governing the proposed framework. We have developed two types of smart contracts, i.e., one we call a local smart contract, and the second one a global smart contract. Moreover, the local smart contract’s main function is to govern the local domain, i.e., inside the organization. A global smart contract is used to govern the global interaction with the system, which means the proposed approach supports scalability and cross-domain applications [31].

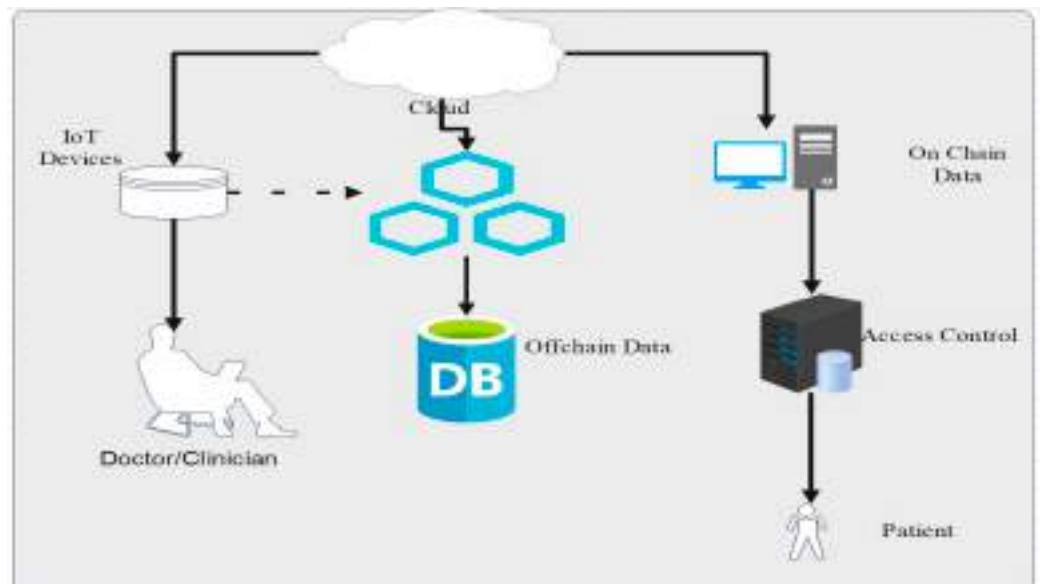


Figure 4. Schematic representation of the proposed smart contracts integration with the cloud.

Consumers regularly use IoT devices to perform transactions from one location to another location using IoT networks. Sending a Web3API transaction requires a contracting state. Using a billfold contract, clients may securely access industrial assets and register large IoT devices. Moreover, the control contract allows the public to inspect and approve the IoT device’s worth [35]. In the proposed TAB-SAPP, smart contracts handle whitelisting,

IoT registration, IoT payment, key computation, and device operation. Consumer signature uses a 256-bit Keccak hash to cope with the external account (ECDSA). The control contract’s private key connects the user, IoT device, and control contract. Here are the steps: In the first phase, an external owner account creates a whitelist. The control contract charges a fee to indicate consumer device access. Anyone who wants to verify a transaction on the blockchain pays a charge. Step two involves the client and IoT device being linked to the external owner account, which facilitates the consideration of consumer needs when fulfilling contractual responsibilities [32]. After successful registration, the IoT gadget pays fees. TAB-SAPP smart contracts handle whitelisting, registration, payment, and key computation. Encrypted elliptic curve signatures with Keccak hash (ECDSA). The control contract’s private key addresses the consumer, IoT device, and control contract. Here are the steps: The contract organization maintains and updates the whitelist using an external owner account. The consumer device control contract specifies the fee request. Using multi-signature to verify a data transaction incurs costs to each party [36]. Customers and devices must be linked to an external owner account to complete IoT registration. The contract organization can accommodate client requests. The IoT gadget then handles the fee payment [37].

3.3. Elliptic Curve for Alternate Key

The proposed approach uses elliptic curve cryptography for key distribution and the interchange of digital signatures, providing more security and trust. Moreover, the use of ring signatures provides trust among the users [38]. The step-by-step mathematical modeling of the proposed model using ring signature and ECC is described below:

$$y^2 \text{ mod } q = (x^3 + ax + b) \text{ mod } q \tag{1}$$

where a, b, x, and y belong to q, and if a point P(x, y) satisfies Equation (1), then the point P(x, y) is a point on an elliptic curve, and the point Q(x, y) is the negative point of P(x, y), i.e., P = -Q. Let points P(x1, y1) and Q(x2, y2) be points on the elliptic curves Eq (a, b) and P*6 = -Q; thus, the line 'l' passes through the points P and Q, and intersects the elliptic curve at the point R0 = (x3, y), the points of R0 symmetrical about the x-axis are R = (x3, y3) and R = P+Q. The points on the elliptic curve Eq (a, b) and the infinite point 0 together form an additive cyclic group of prime order q as follows:

$$Gq = (x, y) : a, b, x, y \text{ belong to } Fq, (x, y) \text{ belong to } Fq \tag{2}$$

$$kP = P + P + \dots + P(k \text{ belong to } Zq) \tag{3}$$

$$S = ((ui + vi) * G), \text{ if } i \tag{4}$$

$$S = (ui G + (vi + wi)) * p \text{ ki}, \tag{5}$$

$$Ri = \sum (ui + wi) * H0(p * ki) \tag{6}$$

$$RI = \sum ui * H0(p * ki) + (vi + wi) * Is \tag{7}$$

$$h = H2(m || r), \tag{8}$$

$$i = \sum H1(h, L1, \dots, Ln, R1, \dots, Rn) \sum s \tag{9}$$

$$i = 1 \text{ Di t} = \sum (u_i + v_i) c_i * s_{k_i} \tag{10}$$

$$D_i t = \sum u_i \text{ if} \tag{11}$$

$$Y_i = d_i * G + c_i * p_{k_i} \tag{12}$$

$$i = d_i * H_0(p_{k_i}) + c_i * I_s \tag{13}$$

∞

$$\sum = H_1(h, Y_1, Y_2, \dots, Y_n, K_1, K_2, \dots, K_n) \tag{14}$$

$\beta = 1$
 n

$$\sum = H_1(h, Y_1, Y_2, \dots, Y_n, \delta_1, \delta_2, \dots, \delta_n) \tag{15}$$

$i = 1$

$$Y_i = d_i * G + c_i * p_{k_i} = u_i * G + (v_i + w_i) * p \text{ Where } k_i = L_i \tag{16}$$

$$Z_i = d_i * H_0(p_{k_i}) + c_i * I_s = u_i * H_0(p_{k_i}) + (v_i + w_i) * I_s \tag{17}$$

When $i = s$, the conversions of (K_i) and (Z_i) are expressed as follows

$$K_i = d_i * G + c_i * p_{k_i} \tag{18}$$

$$Z_i = [(u_i + v_i) - c_i * s_{k_i}] * G + c_i * p_{k_i} \tag{19}$$

$$Z_i = u_i * G + v_i * G, \tag{20}$$

$$\delta_i = d_i * H_0(p_{k_i}) + c_i * I_s \tag{21}$$

$$Z_i = [(u_i + v_i) - c_i * s_{k_i}] * H_0(p_{k_i}) + c_i * s_{k_s} * H_0(p_{k_s}) \tag{22}$$

$$Z_i = u_i * H_0(p_{k_i}) + v_i * H_0(p_{k_i}) \tag{23}$$

Therefore, according to the above relationship, the correctness of the ring signature scheme proposed in this paper is verified as follows

$$C_i = H_1(h, Y_1, Y_2, \dots, Y_s, \dots, Y_n, \delta_1, \delta_2, \dots, \delta_s, \dots, \delta_n) \tag{24}$$

$$C_i = H_1(h, L_1, L_2, \dots, L_s, \dots, L_n, R_1, R_2, \dots, R_s, \dots, R_n) \tag{25}$$

$$C_s = \sum_{i=0}^n C_i \tag{26}$$

Equations (14)–(27) represent the homomorphic encryption of the proposed approach. H_1 represents the homomorphic encryption function that converts the plain text into cipher text. C_s represent the cipher text. Homomorphic encryption provides the facility to encrypt

the data, outsource it to the cloud, and perform any statistical operations over encrypted data. This leads to more privacy and security. In Figure 5, we have explained the process of access control as well as encryption from end to end in the network. The proposed framework uses homomorphic encryption over IoT data in order to outsource to the cloud. Using homomorphic encryption provides the capability to perform any kind of operation over encrypted data. Moreover, the access control checks the user’s attributes such as user name, id, age, gender, location, and height in order to provide access to the EHR or EMR. Moreover, if the user acquires similar attributes, then access is granted through smart contracts; otherwise, access is denied. Figure 6 presents the flow of data through the proposed network. Figure 7 presents the timeline execution through proposed framework.

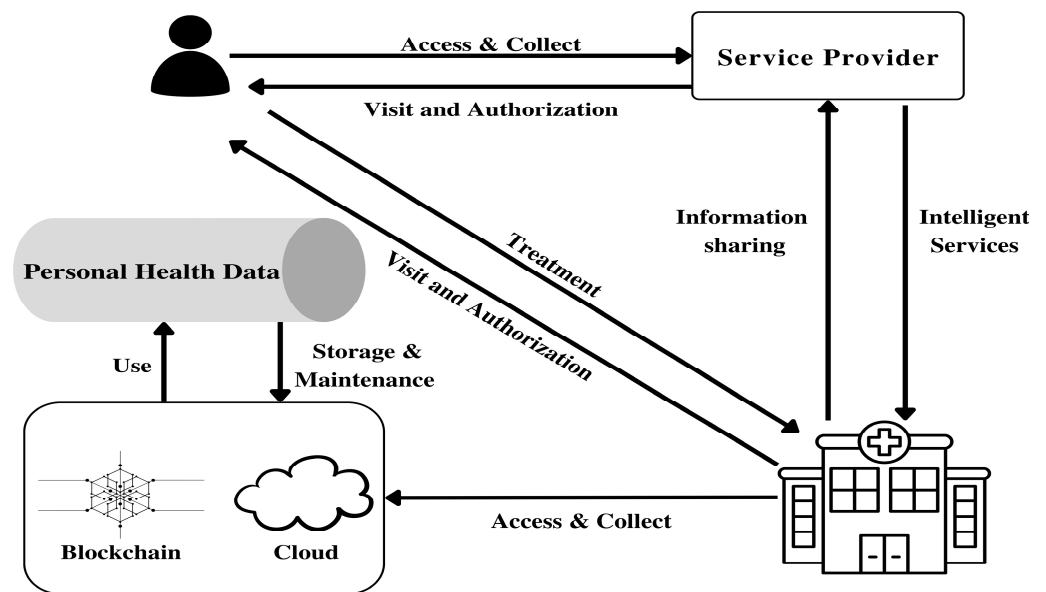


Figure 5. Schematic representation of the proposed access control and outsourcing through blockchain.

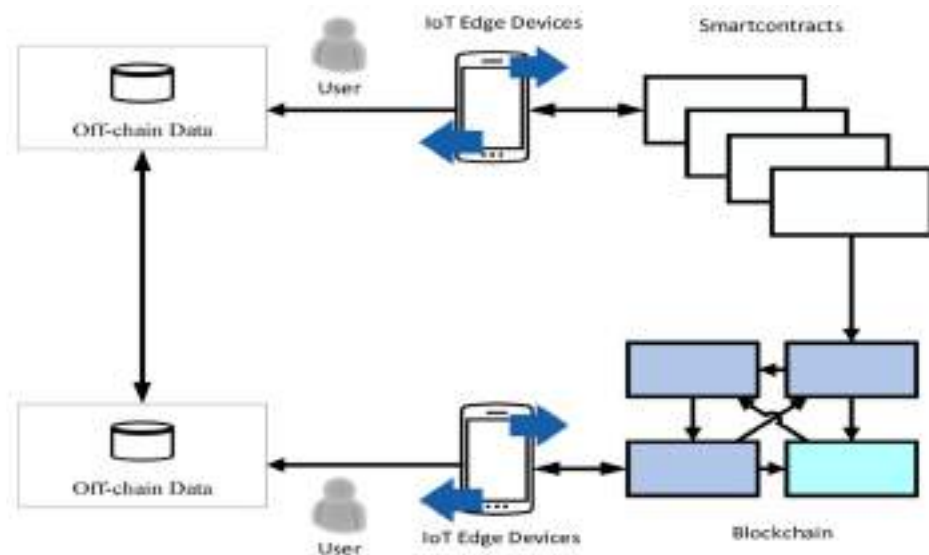


Figure 6. Data flow through proposed network.

3.4. Mathematical Modeling

The mathematical modeling and security protocol design is explained in the following phases. Several phases are required to allow a user to enter into the IoT system in order to read or send data.

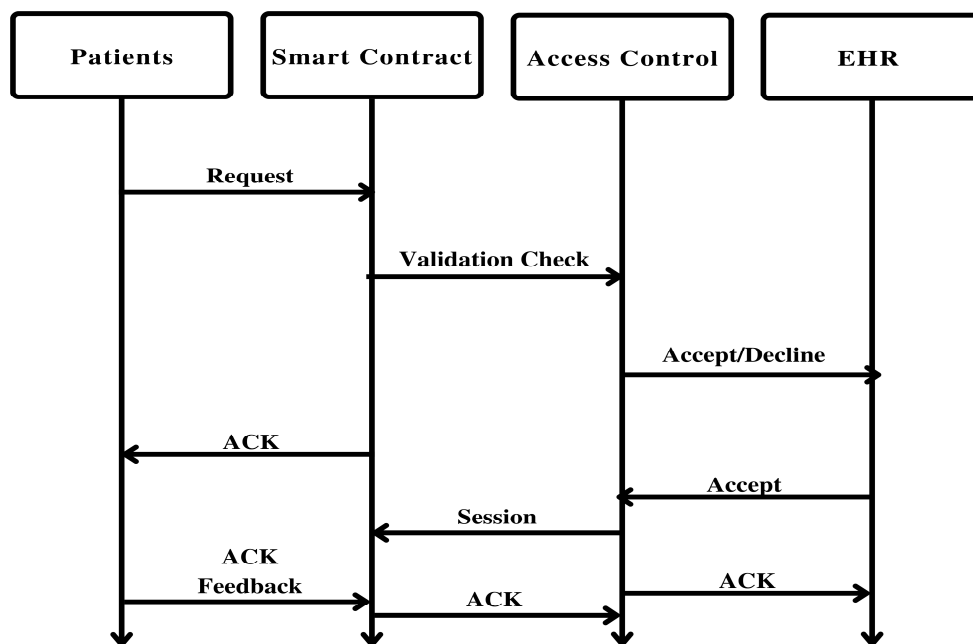


Figure 7. Timeline execution through proposed framework.

3.4.1. Phase 1: System Setup

In the setup phase, the system initializes input parameters for signature creation and user authentication. The procedure of the phase is explained step by step below: Setup (α): Input security parameter (α)

$$\text{let } (G_1) \text{ and } (G_2) \text{ be two multiplicative} \tag{27}$$

$$\text{Assume } (g_1), (g_2) \text{ are two generators } (G_1). \tag{28}$$

3.4.2. Encryption

The transaction is encrypted using attribute-based encryption technique. We used ring signature instead of group signature or AES (Asymmetric Encryption System) for the key exchange. It protects against collusion assaults.

$$[(2 + n)K + 1]C_e x + (2K + 1)C_m + (2K + 1)C_m \tag{29}$$

3.4.3. Decryption

The recipient decrypts the message using both public and private keys. A user with the appropriate attributes can decrypt the cipher text. In the proposed framework, authorized users exchange keys via CA. The decryption time complexity equation is as follows, where K is the number of certificate authorities, n is the message size, and C is the ciphertext.

$$[(n + 1)K + 1]C_p + nKC_e + [3 + (2 + n)K]C_m \tag{30}$$

$$X = Qk \in ICe(C_2, D_k, u), Y = e(C_3, D_1k, u) \tag{31}$$

$$S_k = Q_a k, j \in A_k m e C_k, j, D_j k, u \delta a k, j, A^{\sim} j_m(0) \tag{32}$$

$$m = C_1 X / Y Q k \in IC_S. \tag{33}$$

3.5. Latency

In order to find the total latency of the proposed network it is required to first count latency between node and then calculate the latency of the network. The mathematical model to calculate the total network latency [39] are calculated as follows:

$$T^c = \frac{D_{k,j}}{r_{PB,k}} + T^{co}_{k,j} + \frac{D_{k,j} + h_k}{r_{PB,k}} + {}_{k,j}D \cdot k_{r_{BC,k}} \quad (34)$$

4. Experimental Setup

In order to carry out the experiment, we use a hyperledger fabric tool for blockchain and IoT nodes. During the experiments, the parameters that we recorded and used were the number of nodes, number of rounds, block creation, block digest, encryption time, and access control time. During the simulation results, the system used was core i7 GPU-based and Linux-enabled. Furthermore, for security verification of the proposed model, we used AVISPA [37] and METRE [38] framework in order to verify that the proposed model resist collusion attack and phishing attack.

5. Results and Discussions

This section provides the details of the simulation carried out and the results. Each and every result are discussed in this section. The proposed model was compared with the benchmark model in order to evaluate the performance of the proposed model. Figure 8 depicts the communication overhead in private information retrieval, with several appointment allocation algorithms available in each cell. It can handle the required retrievals by storing in the B+-Tree indexing data structure. Moreover, as compared to SHealth, MedRec, and ECC-Smart solutions, the proposed framework provides minimal communication overhead due to the lightweight authentication system. In this section, we have discussed our proposed simulation results as well as a comparative analysis. The simulation results were conducted using a blockchain tool called hyperledger fabric and deployed it for validation on the Ethereum test net. In this section, we present the simulation results carried out through this research paper. The dataset used is publicly available from UNSW. Figure 8 presents the simulation results of the proposed model, which is compared with the permission-less and private blockchain. Moreover, the comparison is based on the number of transaction counts and a number of nodes. Similarly, from Figure 9, it is very clear that the proposed framework transfer more transaction as compared to the permission-less and private blockchain. This justifies that the proposed framework performs better than the permission-less and private blockchain.

Figure 9 illustrates the simulation results based on the classification of the users using the SVM method. The classification of the users is based on the activities of the users within the system. We used an LSTM deep learning approach to record the previous activities of the users interacting with the system. The proposed approach creates a log of each user's behavior and provides access rights as well as authorization based on the user's behavior.

Figure 10 presents the simulation results based on the displacement of moving sensors connected with the IoT system and the output of the sensor.

Based on the findings in Figure 11, which indicates that the proposed method has enhanced the authentication process through integrating blockchain technology with mobility speed. Through leveraging the immutable and decentralized nature of blockchain technology, coupled with the real-time data capabilities of mobility speed, this will thus ensure that the proposed system is a more secure, efficient, and reliable authentication system. The findings relating to this proposed method offer valuable insights for organizations seeking to optimize their authentication processes in the era of dynamic mobility and digital transformation. The conducted comparative analysis is based on the number of nodes and encryption time with the benchmark models. The proposed framework is compared with the benchmark models which are mentioned on Figure 11.

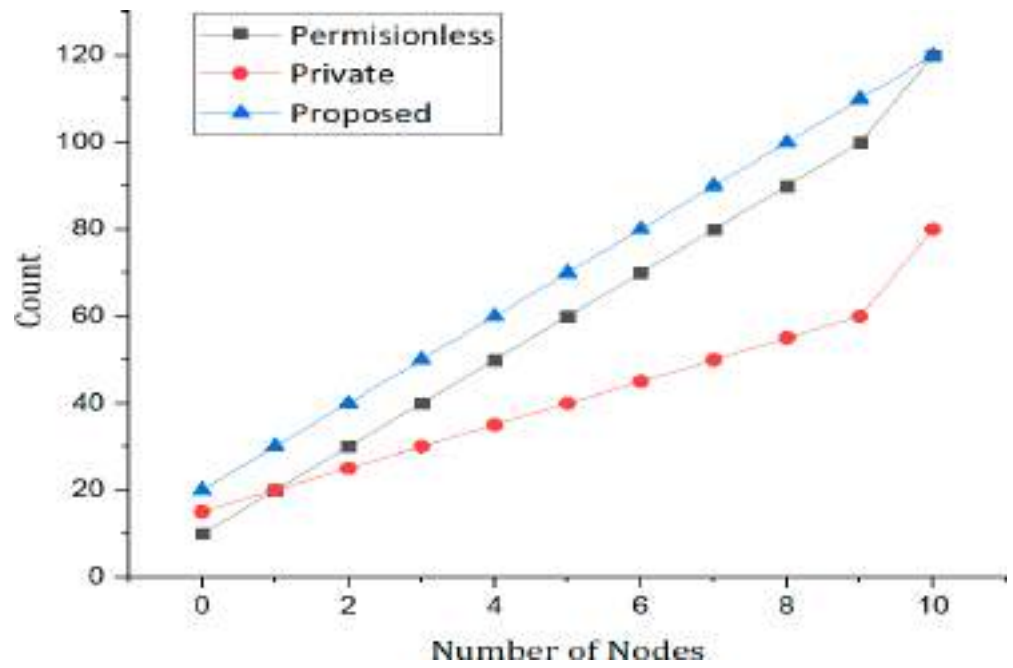


Figure 8. Simulations results based on the number of nodes versus the number of counts.

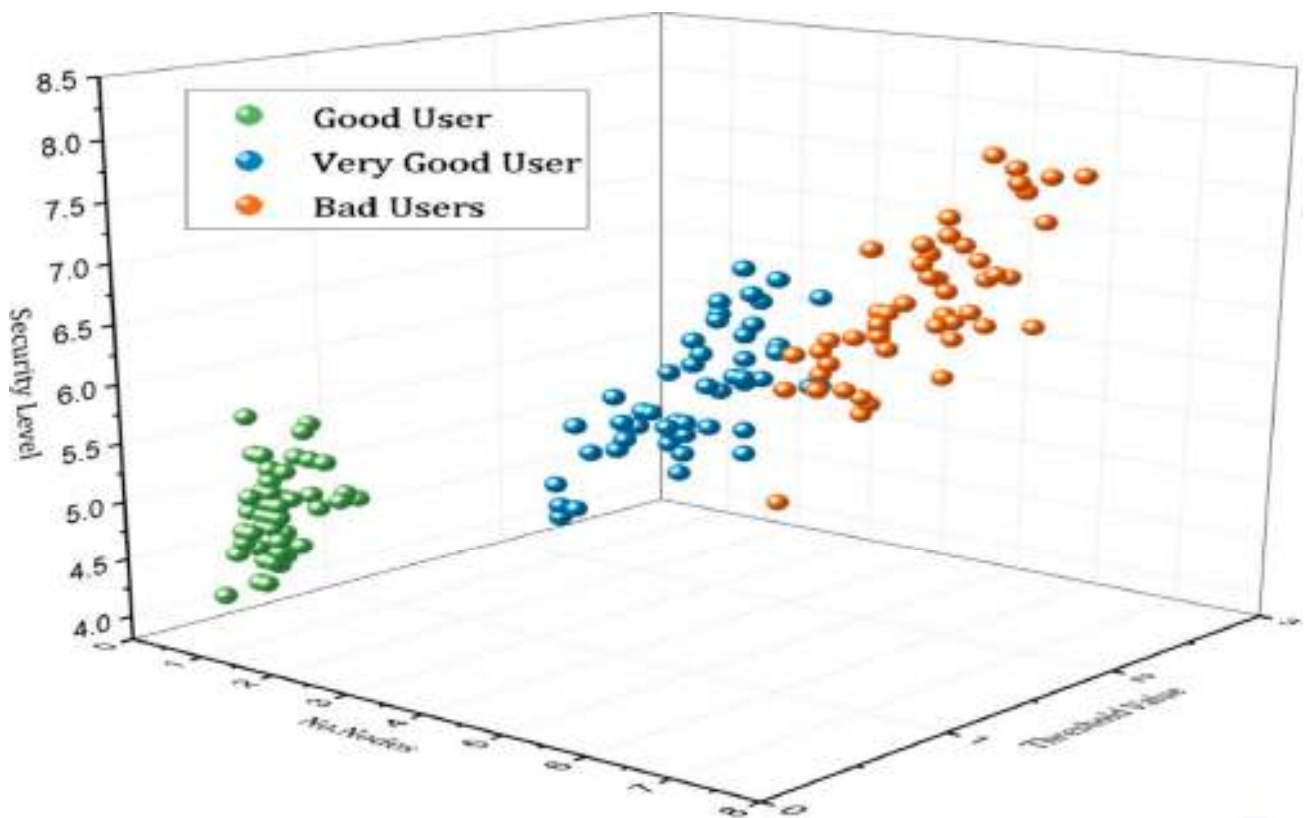


Figure 9. Classification of users based on the behavior and interaction with the system model.

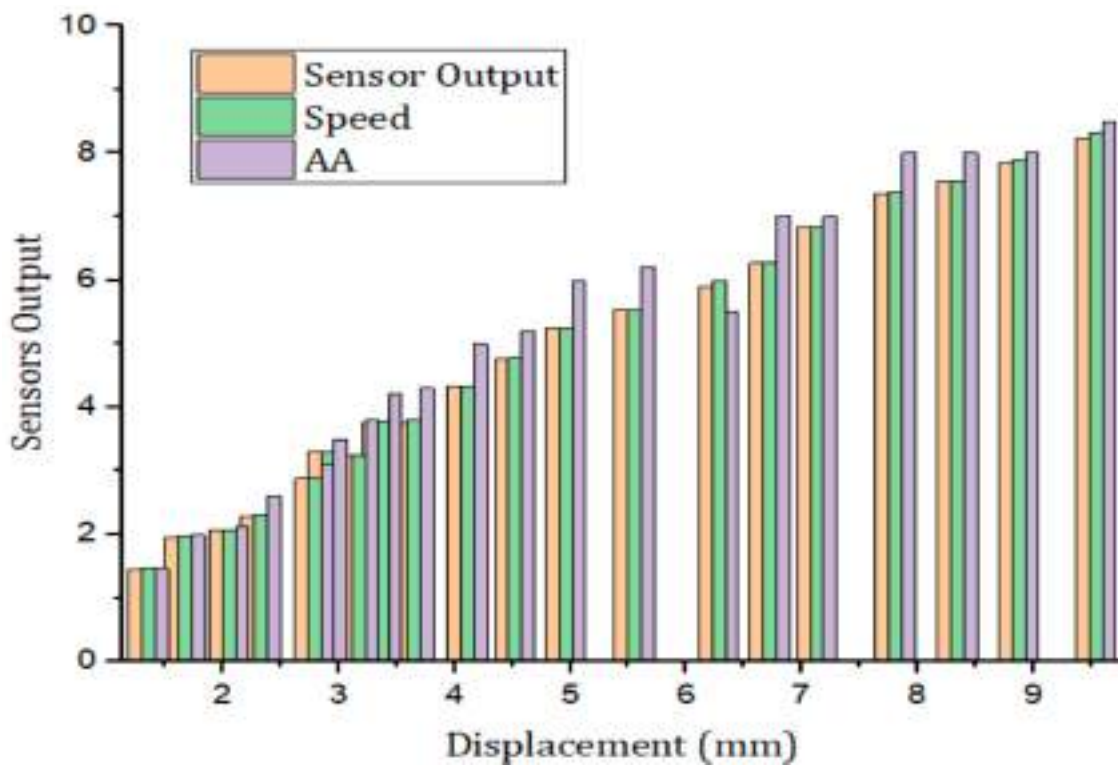


Figure 10. Simulations results based on the number of sensors output nodes.

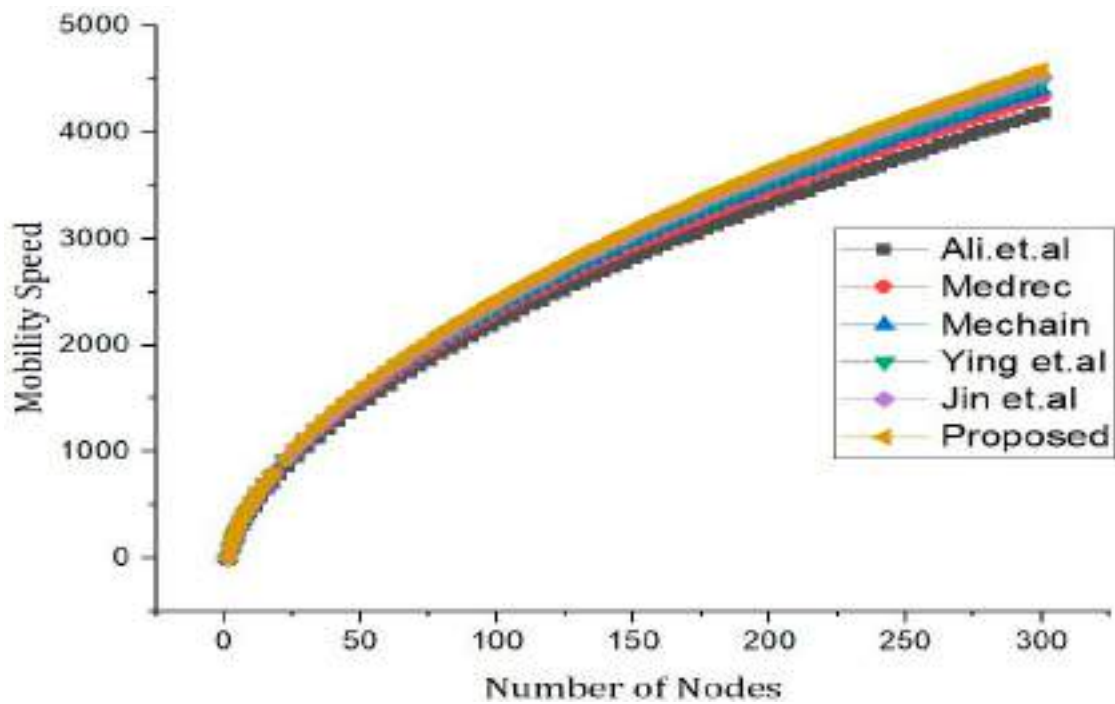


Figure 11. Comparative analysis of the proposed framework versus benchmark model based on the speed and number of nodes.

Figure 12 shows simulation results based on the latency of each node. Moreover, it can be observed that the proposed framework exhibits low latency as compared to the benchmark models. Therefore, the proposed model exhibits efficiency and robustness.

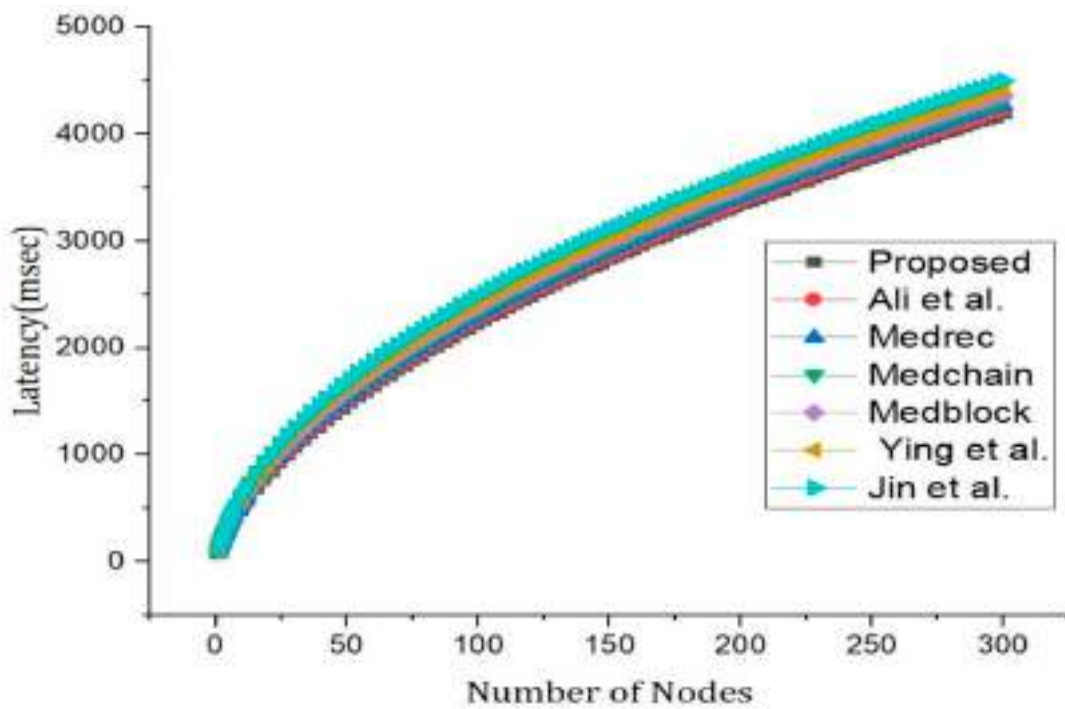


Figure 12. Comparative analysis with the proposed framework versus benchmark model based on the latency and number of nodes.

In Figure 13, the simulation results represent the comparative analysis of the proposed framework versus benchmark models. The comparisons are based on the number of transactions and d2d distance. Moreover, for the same distance between peer nodes, the number of transactions varies.

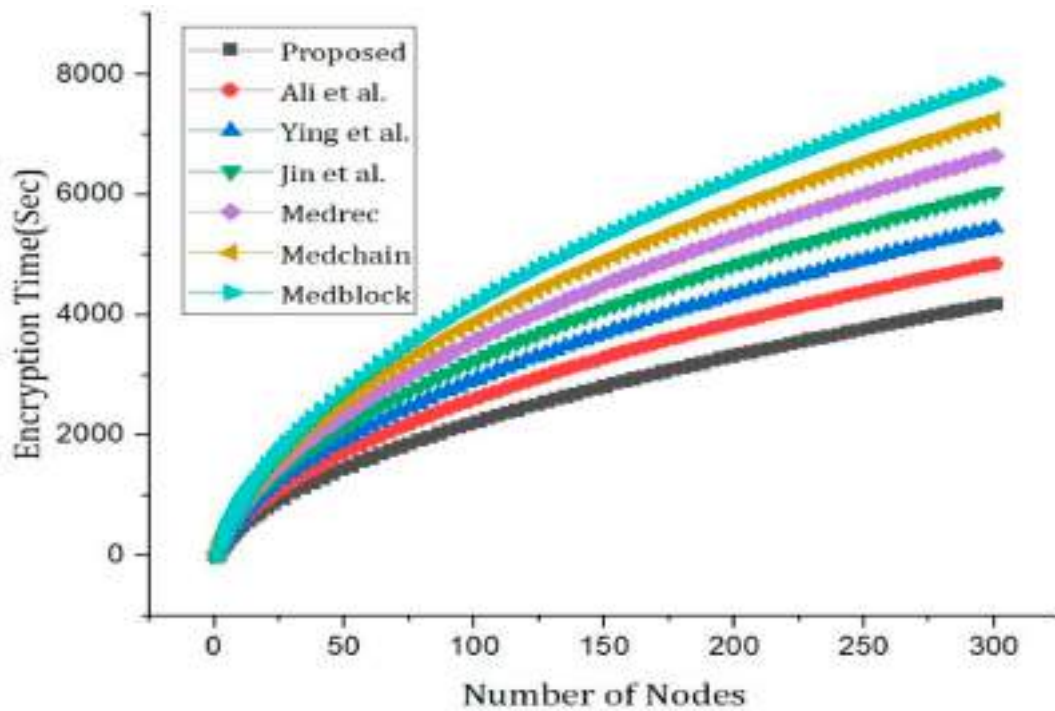


Figure 13. Comparative analysis based on number of nodes versus encryption time.

Moreover, Figure 14 provides the comparative analysis based on the network delay. It can be observed that the network delay for the proposed approach is less as compared to the benchmark approaches.

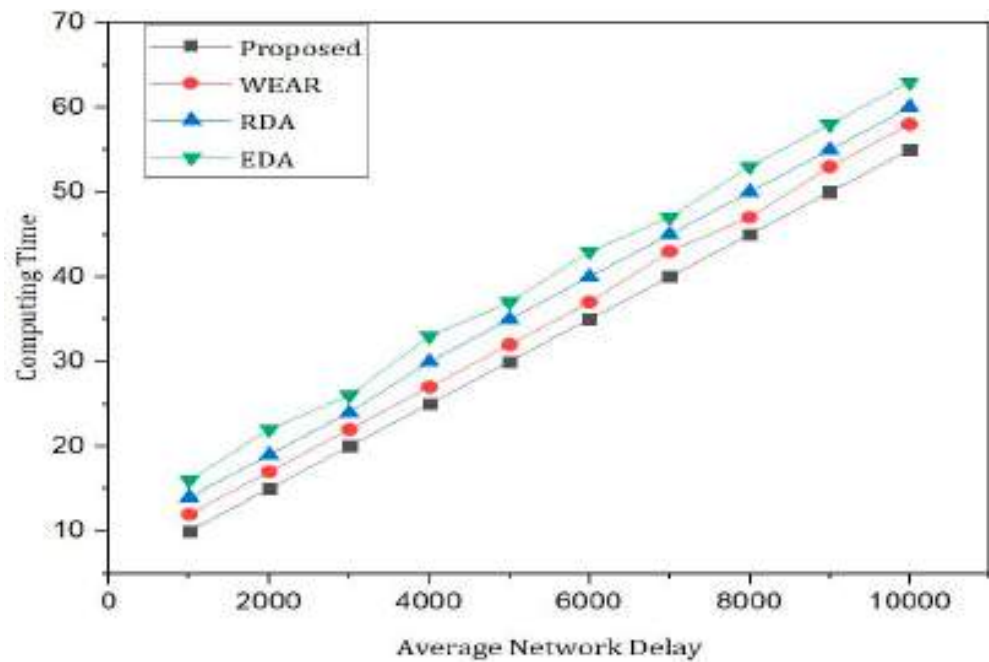


Figure 14. Comparative analysis based on average network delay versus computing time.

The results presented in Figure 15 are recorded to compare the proposed framework with the benchmark models. The parameters to evaluate the proposed framework are distances between two nodes and the number of transactions.

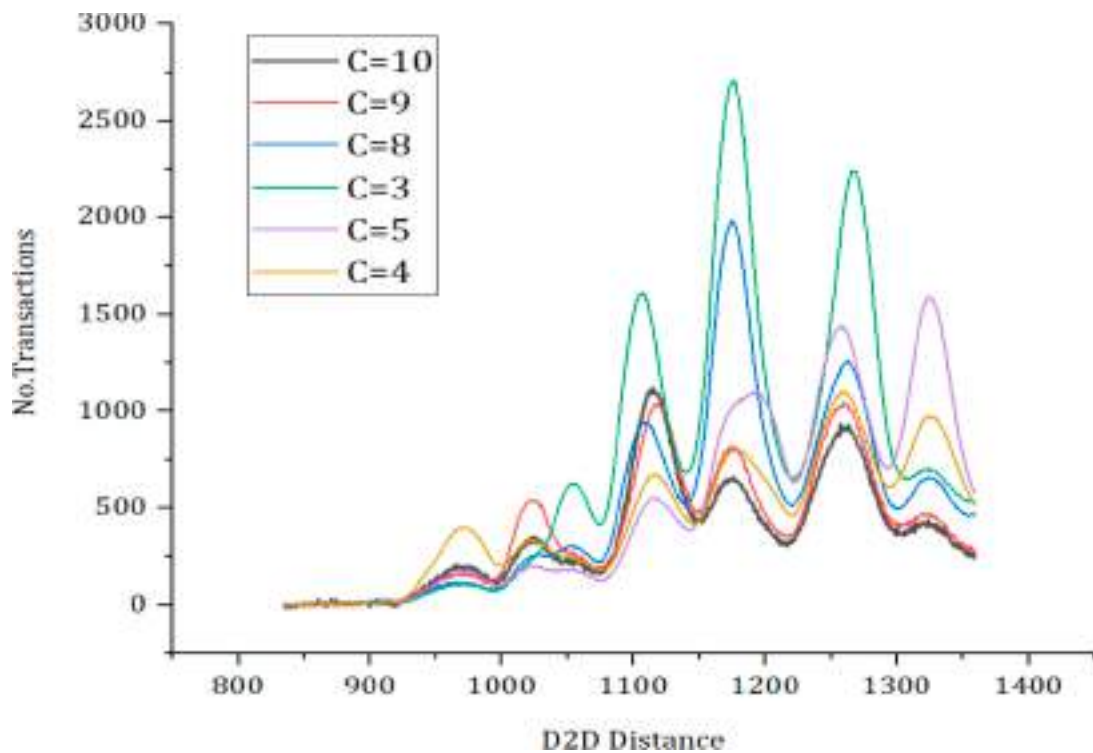


Figure 15. Comparative analysis based on D2D distance versus number of transactions.

Finally, Figure 16 presents the simulation results of the proposed approach, which shows the evaluation based on the number of attributes and the complexity.

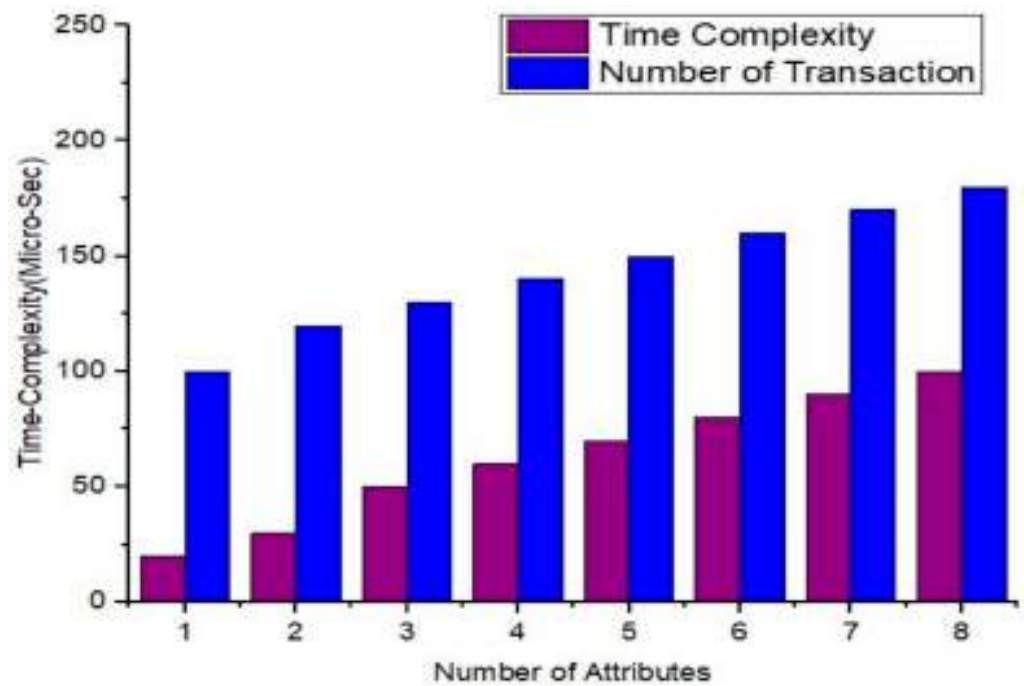


Figure 16. Schematic diagram representing the simulations results based on the number of attributes versus complexity.

Figure 17 presents the comparative analysis of the proposed approach versus the benchmark models based on the number of attributes and execution time.

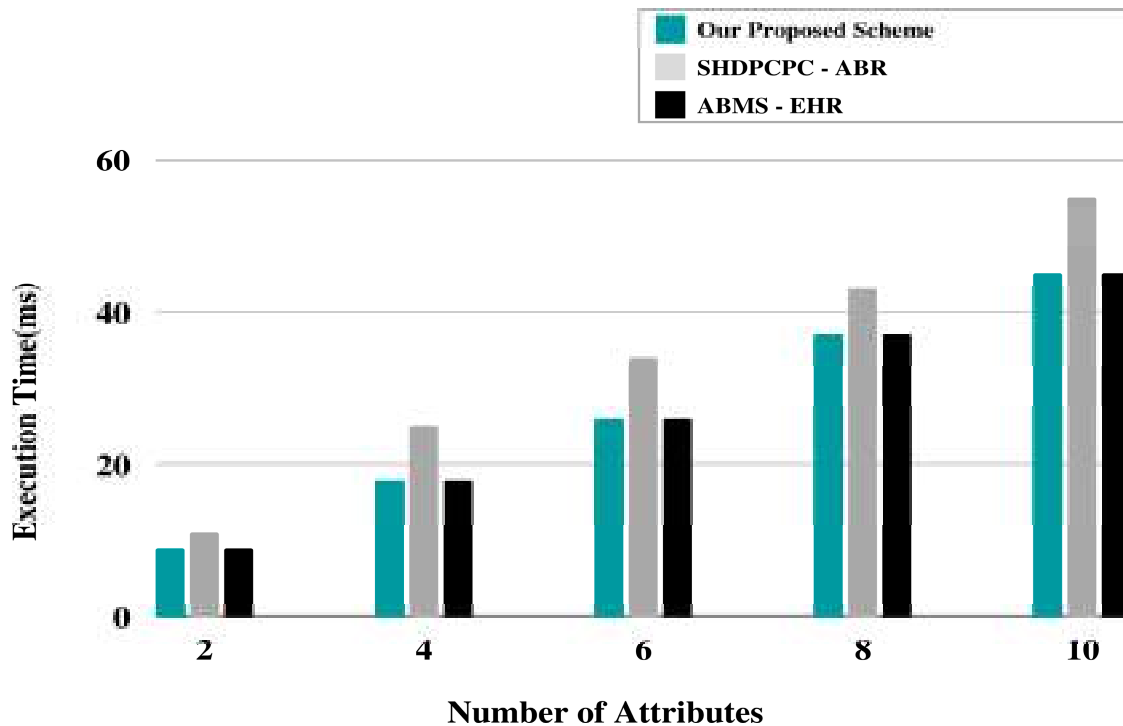


Figure 17. Comparative analysis of the proposed approach versus benchmark models.

The simulation results are based on the number of attributes (X -axis) and execution time (Y -axis). Moreover, it can be observed that using lightweight HE, the proposed approach performs better than the benchmark models in terms of execution for the same number of attributes. In order to evaluate the attack resistance of the proposed framework with the benchmark models, we carried out the comparison shown in Table 2.

Table 2. Comparative analysis of attack resistance.

Models	Collusion Attacks	DoS	DDoS
Medblock	No	No	Yes
Casht	Yes	No	No
Medchain	Yes	No	No
Kasra	Yes	No	No
Proposed	Yes	Yes	Yes

6. Conclusions and Future Works

This study analyses a privacy-preserving authentication system for industrial IoT applications. To reduce processing and communication expenses, the proposed model uses hash evaluation and MAC verification. Massive IoT devices and cloud servers use service deniability to safeguard base-station access and user identities even when linked to open networks. It looked at the transaction's authenticated data blocks randomly. The proposed framework transmission rate is faster than the existing model due to faster calculation, connectivity, and mobility. As a result, the security and performance of computing, communication, and packet delivery has been improved. Moreover, the main objective of the proposed research work is to reduce the latency from end to end. We also compared our proposed framework with the benchmark models. Based on the findings of our study, it was indicated that the proposed method has enhanced the authentication process through integrating blockchain technology with mobility speed. Through leveraging the immutable and decentralized nature of blockchain, coupled with the real-time data capabilities of mobility speed, this will thus ensure the proposed system is a more secure, efficient, and reliable authentication system. These findings of this proposed method offer valuable insights for organizations seeking to optimize their authentication processes in the era of dynamic mobility and digital transformation. The main limitation of our research is that the proposed framework has been developed using only one method, which is based on a permissions-based blockchain that provide data storage optimization and a lightweight authentication mechanism to the users based on smart contracts. In future work, our proposed authentication model can be modified by employing a consensus algorithm to make it more reliable. In the future, we plan to add more advanced algorithms based on deep learning techniques with blockchain technology in order to classify users based on trust. Apart from that, we plan to enhance the proposed approach with a software-defined network and deploy it with 5G technology for quick and efficient response. The future work of this framework can also be integrated with the rescue system in order to receive rescue responses securely and in a short time using blockchain technology.

Author Contributions: Conceptualization, M.A.A.; Methodology, A.K.A.H., S.A.-O., R.S. and A.L.; Software, M.A.A. and M.A.; Validation, A.A.; Formal analysis, A.K.A.H., A.L. and M.A.; Investigation, S.A.-O.; Resources, M.A.A. and R.S.; Data curation, A.K.A.H., S.A.-O., A.L. and M.A.; Writing—original draft, A.A.; Writing—review & editing, R.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported through the Annual Funding track by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Project No. Grant No. 3898) and Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R136), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Data Availability Statement: Not Applicable.

Conflicts of Interest: All authors declare no conflict of interest.

References

1. Siam, A.I.; Almaiah, M.A.; Al-Zahrani, A.; Elazm, A.A.; El Banby, G.M.; El-Shafai, W.; El-Samie, F.E.A.; El-Bahnasawy, N.A. Secure Health Monitoring Communication Systems Based on IoT and Cloud Computing for Medical Emergency Applications. *Comput. Intell. Neurosci.* **2021**, *2021*, 8016525. [[CrossRef](#)]
2. Ali, A.; Pasha, M.F.; Fang, O.H.; Khan, R.; Almaiah, M.A.; KAl Hwaitat, A. Big data based smart blockchain for information retrieval in privacy-preserving healthcare system. In *Big Data Intelligence for Smart Applications*; Springer International Publishing: Cham, Switzerland, 2022; pp. 279–296.
3. Altulaihan, E.; Almaiah, M.A.; Aljughaiman, A. Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions. *Electronics* **2022**, *11*, 3330.
4. Hasnain, M.; Pasha, M.F.; Ghani, I.; Mehboob, B.; Imran, M.; Ali, A. *Benchmark Dataset Selection of Web Services Technologies: A Factor Analysis*; IEEE Access: Piscataway, NJ, USA, 2020; Volume 8, pp. 53649–53665.
5. Ali, A.; Rahim, H.A.; Pasha, M.F.; Dowsley, R.; Masud, M.; Ali, J.; Baz, M. Security, Privacy, and Reliability in Digital Healthcare Systems Using Blockchain. *Electronics* **2021**, *10*, 2034.
6. Almaiah, M.A.; Hajje, F.; Ali, A.; Pasha, M.F.; Almomani, O. An AI-Enabled Hybrid Lightweight Authentication Model for Digital Healthcare Using Industrial Internet of Things Cyber-Physical Systems. *Sensors* **2022**, *22*, 1448. [[PubMed](#)]
7. Yazdinejad, A.; Dehghantanha, A.; Parizi, R.M.; Srivastava, G.; Karimipour, H. Secure Intelligent Fuzzy Blockchain Framework: Effective Threat Detection in IoT Networks. *Comput. Ind.* **2023**, *144*, 103801. [[CrossRef](#)]
8. Hameed, K.; Ali, A.; Naqvi, M.H.; Jabbar, M.; Junaid, M.; Haider, A. Resource management in operating systems—a survey of scheduling algorithms. In *Proceedings of the International Conference on Innovative Computing (ICIC)*, Lanzhou, China, 2–5 August 2016; Volume 1.
9. Singh, H.; Ahmed, Z.; Khare, M.D.; Bhuvana, J. An IoT and Blockchain-Based Secure Medical Care Framework Using Deep Learning and Nature-Inspired Algorithms. *Int. J. Intell. Syst. Appl. Eng.* **2023**, *11*, 183–191.
10. Kim, H.; Kim, S.-H.; Hwang, J.Y.; Seo, C. Efficient Privacy-Preserving Machine Learning for Blockchain Network. *IEEE Access* **2019**, *7*, 136481–136495.
11. Sharma, P.; Namasudra, S.; Crespo, R.G.; Parra-Fuente, J.; Trivedi, M.C. EHDHE: Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain. *Inf. Sci.* **2023**, *629*, 703–718.
12. Almadani, M.S.; Alotaibi, S.; Alsobhi, H.; Hussain, O.K.; Hussain, F.K. Blockchain-based multi-factor authentication: A systematic literature review. *Internet Things* **2023**, *23*, 100844. [[CrossRef](#)]
13. Kumar, P.; Kumar, R.; Gupta, G.P.; Tripathi, R.; Jolfaei, A.; Islam, A.N. A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system. *J. Parallel Distrib. Comput.* **2023**, *172*, 69–83. [[CrossRef](#)]
14. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Choo, K.-K.R. P4-to-blockchain: A secure blockchain-enabled packet parser for software defined networking. *Comput. Secur.* **2020**, *88*, 101629. [[CrossRef](#)]
15. Sharma, P.C.; Mahmood, R.; Raja, H.; Yadav, N.S.; Gupta, B.B.; Arya, V. Secure authentication and privacy-preserving blockchain for industrial internet of things. *Comput. Electr. Eng.* **2023**, *108*, 108703. [[CrossRef](#)]
16. Jiang, S.; Cao, J.; Wu, H.; Yang, Y. Fairness-Based Packing of Industrial IoT Data in Permissioned Blockchains. *IEEE Trans. Ind. Inform.* **2020**, *17*, 7639–7649. [[CrossRef](#)]
17. Bordel, B.; Alcarria, R.; Robles, T. *A Blockchain Ledger for Securing Isolated Ambient Intelligence Deployments Using Reputation and Information Theory Metrics*; Wireless Networks: New York, NY, USA, 2023; pp. 1–7.
18. Selvarajan, S.; Srivastava, G.; Khadidos, A.O.; Khadidos, A.O.; Baza, M.; Alshehri, A.; Lin, J.C.-W. An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems. *J. Cloud Comput.* **2023**, *12*, 38. [[CrossRef](#)] [[PubMed](#)]
19. Lacity, M.C. Addressing Key Challenges to Making Enterprise Blockchain Applications a Reality. *J. Mis. Q. Exec.* **2018**, *17*, 3.
20. Sengupta, J.; Ruj, S.; Das Bit, S. A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. *J. Netw. Comput. Appl.* **2020**, *149*, 102481. [[CrossRef](#)]
21. Pajooh, H.; Rashid, M.; Alam, F.; Demidenko, S. Multi-Layer Blockchain-Based Security Architecture for Internet of Things. *Sensors* **2021**, *21*, 772. [[CrossRef](#)]
22. Peng, C.; Wu, C.; Gao, L.; Zhang, J.; Yau, K.-L.A.; Ji, Y. Blockchain for Vehicular Internet of Things: Recent Advances and Open Issues. *Sensors* **2020**, *20*, 5079. [[CrossRef](#)]
23. Esposito, C.; De Santis, A.; Tortora, G.; Chang, H.; Choo, K.-K.R. Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? *IEEE Cloud Comput.* **2018**, *5*, 31–37. [[CrossRef](#)]
24. Patel, V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Inform. J.* **2018**, *25*, 1398–1411. [[CrossRef](#)] [[PubMed](#)]
25. Kim, T.M.; Lee, S.-J.; Chang, D.-J.; Koo, J.; Kim, T.; Yoon, K.-H.; Choi, I.-Y. DynamiChain: Development of Medical Blockchain Ecosystem Based on Dynamic Consent System. *Appl. Sci.* **2021**, *11*, 1612. [[CrossRef](#)]

26. Hang, L.; Kim, D.-H. Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity. *Sensors* **2019**, *19*, 2228. [[CrossRef](#)] [[PubMed](#)]
27. Figorilli, S.; Antonucci, F.; Costa, C.; Pallottino, F.; Raso, L.; Castiglione, M.; Pinci, E.; Del Vecchio, D.; Colle, G.; Proto, A.R.; et al. A Blockchain Implementation Prototype for the Electronic Open Source Traceability of Wood along the Whole Supply Chain. *Sensors* **2018**, *18*, 3133. [[CrossRef](#)]
28. Zhu, X.; Badr, Y. Identity management systems for the internet of things: A survey towards blockchain solutions. *Sensors* **2018**, *18*, 4215. [[CrossRef](#)]
29. Jia, X.; Hu, N.; Su, S.; Yin, S.; Zhao, Y.; Cheng, X.; Zhang, C. IRBA: An Identity-Based Cross-Domain Authentication Scheme for the Internet of Things. *Electronics* **2020**, *9*, 634. [[CrossRef](#)]
30. Ali, A.; Rahim, H.; Ali, J.; Pasha, M.F.; Masud, M.; Rehman, A.U.; Chen, C.; Baz, M. A Novel Secure Blockchain Framework for Accessing Electronic Health Records Using Multiple Certificate Authority. *Appl. Sci.* **2021**, *11*, 9999. [[CrossRef](#)]
31. Lin, Z.; Niu, H.; An, K.; Wang, Y.; Zheng, G.; Chatzinotas, S.; Hu, Y. Refracting RIS-Aided Hybrid Satellite-Terrestrial Relay Networks: Joint Beamforming Design and Optimization. *IEEE Trans. Aerosp. Electron. Syst.* **2022**, *58*, 3717–3724. [[CrossRef](#)]
32. Lin, Z.; An, K.; Niu, H.; Hu, Y.; Chatzinotas, S.; Zheng, G.; Wang, J. SLNR-based Secure Energy Efficient Beamforming in Multibeam Satellite Systems. *IEEE Trans. Aerosp. Electron. Syst.* **2022**, *59*, 2085–2088. [[CrossRef](#)]
33. Niu, H.; Lin, Z.; Chu, Z.; Zhu, Z.; Xiao, P.; Nguyen, H.X.; Lee, I.; Al-Dhahir, N. Joint Beamforming Design for Secure RIS-Assisted IoT Networks. *IEEE Internet Things J.* **2022**, *10*, 1628–1641. [[CrossRef](#)]
34. Lin, Z.; Lin, M.; de Cola, T.; Wang, J.-B.; Zhu, W.-P.; Cheng, J. Supporting IoT With Rate-Splitting Multiple Access in Satellite and Aerial-Integrated Networks. *IEEE Internet Things J.* **2021**, *8*, 11123–11134. [[CrossRef](#)]
35. Tan, L.; Shi, N.; Yu, K.; Alokaily, M.; Jararweh, Y. A Blockchain-empowered Access Control Framework for Smart Devices in Green Internet of Things. *ACM Trans. Internet Technol.* **2021**, *21*, 1–20. [[CrossRef](#)]
36. Yu, K.; Tan, L.; Yang, C.; Choo, K.-K.R.; Bashir, A.K.; Rodrigues, J.J.P.C.; Sato, T. A Blockchain-Based Shamir's Threshold Cryptography Scheme for Data Protection in Industrial Internet of Things Settings. *IEEE Internet Things J.* **2021**, *9*, 8154–8167. [[CrossRef](#)]
37. Peng, Z.; Xu, J.; Hu, H.; Chen, L.; Kong, H. BlockShare: A Blockchain empowered system for privacy-preserving verifiable data sharing. *Bull. IEEE Comput. Soc. Tech. Comm. Data Eng.* **2022**, *1*, 14–24.
38. Peng, Z.; Zhang, Y.; Xu, Q.; Liu, H.; Gao, Y.; Li, X.; Yu, G. NeuChain: A fast permissioned blockchain system with deterministic ordering. *Proc. VLDB Endow.* **2022**, *15*, 2585–2598. [[CrossRef](#)]
39. Peng, Z.; Huang, J.; Wang, H.; Wang, S.; Chu, X.; Zhang, X.; Chen, L.; Huang, X.; Fu, X.; Guo, Y.; et al. BU-trace: A permissionless mobile system for privacy-preserving intelligent contact tracing. In *International Conference on Database Systems for Advanced Applications*; Springer: Cham, Switzerland, 2021; pp. 381–397.
40. Ruan, P.; Chen, G.; Dinh, T.T.A.; Lin, Q.; Ooi, B.C.; Zhang, M. Fine-grained, secure and efficient data provenance on blockchain systems. *Proc. VLDB Endow.* **2019**, *12*, 975–9888. [[CrossRef](#)]
41. Wang, H.; Xu, C.; Zhang, C.; Xu, J.; Peng, Z.; Pei, J. vChain+: Optimizing Verifiable Blockchain Boolean Range Queries. In *Proceedings of the 2022 IEEE 38th International Conference on Data Engineering (ICDE)*, Kuala Lumpur, Malaysia, 9–12 May 2022; pp. 1927–1940.
42. Ruan, P.; Dinh, T.T.A.; Lin, Q.; Zhang, M.; Chen, G.; Ooi, B.C. Revealing Every Story of Data in Blockchain Systems. *ACM SIGMOD Rec.* **2020**, *49*, 70–77. [[CrossRef](#)]
43. Saadeh, M.; Sleit, A.; Qatawneh, M.; Almobaideen, W. Authentication techniques for the internet of things: A survey. In *Proceedings of the 2016 Cybersecurity and Cyberforensics Conference (CCC)*, Amman, Jordan, 2–4 August 2016; pp. 28–34.
44. AbuAlghanam, O.; Qatawneh, M.; Almobaideen, W.; Saadeh, M. A new hierarchical architecture and protocol for key distribution in the context of IoT-based smart cities. *J. Inf. Secur. Appl.* **2022**, *67*, 103173. [[CrossRef](#)]
45. Altarawneh, M.; Qatawneh, M.; Almobaideen, W. Overview of Applied Data Analytic Mechanisms and Approaches Using Permissioned Blockchains. *Int. J. Adv. Sci. Eng. Inf. Technol.* **2022**, *12*, 42–52. [[CrossRef](#)]
46. Qatawneh, M.; Almobaideen, W.; AbuAlghanam, O. Challenges of Blockchain Technology in Context Internet of Things: A Survey. *Int. J. Comput. Appl.* **2020**, *175*, 13–20. [[CrossRef](#)]
47. Abualghanam, O.R.; Qatawneh, M.O.; Almobaideen, W.E. A survey of key distribution in the context of internet of things. *J. Theor. Appl. Inf. Technol.* **2019**, *97*, 3217–3241.
48. Adil, M.; Almaiah, M.A.; Alsayed, A.O.; Almomani, O. An Anonymous Channel Categorization Scheme of Edge Nodes to Detect Jamming Attacks in Wireless Sensor Networks. *Sensors* **2020**, *20*, 2311. [[CrossRef](#)] [[PubMed](#)]
49. Adil, M.; Khan, R.; Almaiah, M.A.; Al-Zahrani, M.; Zakarya, M.; Amjad, M.S.; Ahmed, R. MAC-AODV Based Mutual Authentication Scheme for Constraint Oriented Networks. *IEEE Access* **2020**, *8*, 44459–44469. [[CrossRef](#)]
50. Adil, M.; Khan, R.; Ali, J.; Roh, B.-H.; Ta, Q.T.H.; Almaiah, M.A. An Energy Proficient Load Balancing Routing Scheme for Wireless Sensor Networks to Maximize Their Lifespan in an Operational Environment. *IEEE Access* **2020**, *8*, 163209–163224. [[CrossRef](#)]
51. Adil, M.; Khan, R.; Almaiah, M.A.; Binsawad, M.; Ali, J.; Al Saaidah, A.; Ta, Q.T.H. An Efficient Load Balancing Scheme of Energy Gauge Nodes to Maximize the Lifespan of Constraint Oriented Networks. *IEEE Access* **2020**, *8*, 148510–148527. [[CrossRef](#)]

52. Rahman, H.U.; Almaiah, M.A.; Khan, M.Z.; Khan, A.; Raza, M.; Al-Zahrani, M.; Almomani, O.; Khan, R. Improving Energy Efficiency With Content-Based Adaptive and Dynamic Scheduling in Wireless Sensor Networks. *IEEE Access* **2020**, *8*, 176495–176520.
53. Tatnall, A. Editorial for EAIT issue 2, 2019. *Educ. Inf. Technol.* **2019**, *24*, 953–962. [[CrossRef](#)]
54. Almaiah, M.A.; Al-Zahrani, A.; Almomani, O.; Alhwaitat, A.K. Classification of cyber security threats on mobile devices and applications. In *Artificial Intelligence and Blockchain for Future Cybersecurity Applications*; Springer: Cham, Switzerland, 2021; pp. 107–123.
55. Sultana, T.; Almogren, A.; Akbar, M.; Zuair, M.; Ullah, I.; Javaid, N. Data Sharing System Integrating Access Control Mechanism using Blockchain-Based Smart Contracts for IoT Devices. *Appl. Sci.* **2020**, *10*, 488. [[CrossRef](#)]
56. Shen, B.; Guo, J.; Yang, Y. MedChain: Efficient Healthcare Data Sharing via Blockchain. *Appl. Sci.* **2019**, *9*, 1207. [[CrossRef](#)]
57. Sharma, A.; Sarishma; Tomar, R.; Chilamkurti, N.; Kim, B.-G. Blockchain Based Smart Contracts for Internet of Medical Things in e-Healthcare. *J. Electron.* **2020**, *9*, 1609. [[CrossRef](#)]
58. Alam Khan, F.; Asif, M.; Ahmad, A.; Alharbi, M.; Aljuaid, H. Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development. *Sustain. Cities Soc.* **2020**, *55*, 102018. [[CrossRef](#)]
59. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. *Sensors* **2020**, *19*, 326. [[CrossRef](#)]
60. Alamer, M.; Almaiah, M.A. Cybersecurity in Smart City: A systematic mapping study. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; pp. 719–724.
61. Rath, V.K.; Chaudhary, V.; Rajput, N.K.; Ahuja, B.; Jaiswal, A.K.; Gupta, D.; Elhoseny, M.; Hammoudeh, M. A blockchain-enabled multi domain edge computing orchestrator. *J. IEEE Internet Things Mag.* **2020**, *3*, 30–36. [[CrossRef](#)]
62. Al Hwaitat, A.K.; Almaiah, M.A.; Almomani, O.; Al-Zahrani, M.; Al-Sayed, R.M.; Asaifi, R.M.; Adhim, K.K.; Althunibat, A.; Alsaaidah, A. Improved security particle swarm optimization (PSO) algorithm to detect radio jamming attacks in mobile networks. *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11*, 4. [[CrossRef](#)]
63. Ali, A.; Almaiah, M.A.; Hajje, F.; Pasha, M.F.; Fang, O.H.; Khan, R.; Teo, J.; Zakarya, M. An Industrial IoT-Based Blockchain-Enabled Secure Searchable Encryption Approach for Healthcare Systems Using Neural Network. *Sensors* **2022**, *22*, 572. [[CrossRef](#)] [[PubMed](#)]
64. Almaiah, M.A.; Dawahdeh, Z.; Almomani, O.; Alsaaidah, A.; Al-Khasawneh, A.; Khawatreh, S. A new hybrid text encryption approach over mobile ad hoc network. *Int. J. Electr. Comput. Eng. IJECE* **2020**, *10*, 6461–6471. [[CrossRef](#)]
65. Nkenyereye, L.; Adhi Tama, B.; Shahzad, M.K.; Choi, Y.-H. Secure and blockchain-based emergency driven message protocol for 5G enabled vehicular edge computing. *Sensors* **2020**, *20*, 154. [[CrossRef](#)]
66. Feng, C.; Yu, K.; Bashir, A.K.; Al-Otaibi, Y.D.; Lu, Y.; Chen, S.; Zhang, D. Efficient and secure data sharing for 5G flying drones: A blockchain-enabled approach. *IEEE Netw.* **2021**, *35*, 130–137. [[CrossRef](#)]
67. Khujamatov, K.; Reypnazarov, E.; Akhmedov, N.; Khasanov, D. Blockchain for 5G Healthcare architecture. In Proceedings of the 2020 International Conference on Information Science and Communications Technologies (ICISCT), Karachi, Pakistan, 8–9 February 2020; pp. 1–5.
68. Almaiah, M.A. A new scheme for detecting malicious attacks in wireless sensor networks based on blockchain technology. In *Artificial Intelligence and Blockchain for Future Cybersecurity Applications*; Springer: Cham, Switzerland, 2021; pp. 217–234.
69. Bubukayr, M.A.; Almaiah, M.A. Cybersecurity concerns in smart-phones and applications: A survey. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14 July 2021; pp. 725–731.
70. Almaiah, M.A.; Hajje, F.; Ali, A.; Pasha, M.F.; Almomani, O. A Novel Hybrid Trustworthy Decentralized Authentication and Data Preservation Model for Digital Healthcare IoT Based CPS. *Sensors* **2022**, *22*, 1448. [[CrossRef](#)]
71. Al Nafea, R.; Almaiah, M.A. Cyber security threats in cloud: Literature review. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14 July 2021; pp. 779–786.
72. Almomani, O.; Almaiah, M.A.; Alsaaidah, A.; Smadi, S.; Mohammad, A.H.; Althunibat, A. Machine learning classifiers for network intrusion detection system: Comparative study. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; pp. 440–445.
73. Almaiah, M.A.; Ali, A.; Hajje, F.; Pasha, M.F.; Alohal, M.A. A Lightweight Hybrid Deep Learning Privacy Preserving Model for FC-Based Industrial Internet of Medical Things. *Sensors* **2022**, *22*, 2112. [[CrossRef](#)]
74. Vivekanandan, M.; Sastry, V.N. *BIDAPSCA5G: Blockchain Based Internet of Things (IoT) Device to Device Authentication Protocol for Smart City Applications Using 5G Technology Peer-to-Peer Networking and Applications*; Springer: Cham, Switzerland, 2021; Volume 14, pp. 403–419.
75. Gao, J.; Agyekum, K.O.O.; Sifah, E.B.; Acheampong, K.N.; Xia, Q.; Du, X.; Guizani, M.; Xia, H. A blockchain-SDN-enabled Internet of vehicles environment for fog computing and 5G networks. *IEEE Internet Things J.* **2019**, *7*, 4278–4291. [[CrossRef](#)]
76. Zhou, S.; Huang, H.; Chen, W.; Zhou, P.; Zheng, Z.; Guo, S. Pirate: A blockchain-based secure framework of distributed machine learning in 5g networks. *IEEE Netw.* **2020**, *34*, 84–91. [[CrossRef](#)]
77. Zhang, Y.; Wang, K.; Moustafa, H.; Wang, S.; Zhang, K. Guest Editorial: Blockchain and AI for Beyond 5G Networks. *IEEE Netw.* **2020**, *34*, 22–23. [[CrossRef](#)]
78. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Choo, K.-K.R. Blockchain-enabled authentication handover with efficient privacy protection in SDN-based 5G networks. *IEEE Trans. Netw. Sci. Eng.* **2019**, *8*, 1120–1132. [[CrossRef](#)]

79. Zhao, Y.; Zhao, J.; Zhai, W.; Sun, S.; Niyato, D.; Lam, K. *A Survey of 6G Wireless Communications: Emerging Technologies Future of Information and Communication Conference*; Springer: Cham, Switzerland, 2021; pp. 150–170.
80. Bhattacharya, P.; Tanwar, S.; Shah, R.; Ladha, A. Mobile edge computing-enabled blockchain framework—A survey. In *Proceedings of the ICRIC 2019*; Springer: Cham, Switzerland, 2020; pp. 797–809.
81. *Blockchain and 5G-Enabled Internet of Things: Background and Preliminaries Blockchain for 5G-Enabled IoT*; Springer: Cham, Switzerland, 2021; pp. 3–31.
82. Mistry, I.; Tanwar, S.; Tyagi, S.; Kumar, N. Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. *Mech. Syst. Signal Process.* **2020**, *135*, 106382. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.