sustainability

MDPI

Article

A Lightweight Authentication and Authorization Framework for Blockchain-Enabled IoT Network in Health-Informatics

Muhammad Tahir [1], Muhammad Sardaraz [1,*], Shakoor Muhammad [2] and Muhammad Saud Khan [1]

[1] Department of Computer Science, COMSATS University Islamabad, Attock Campus, Punjab 43600, Pakistan; m_tahir@cuiatk.edu.pk (M.T.); saud_khan@ciit-attock.edu.pk (M.S.K.)

[2] Department of Mathematics, Abdulwali Khan University, Mardan, Khyber Pakhtunkhwa 23200, Pakistan; shakoormath@gmail.com

* Correspondence: sardaraz@cuiatk.edu.pk; Tel.: +92-57-9049311

Received: 22 July 2020; Accepted: 17 August 2020; Published: 26 August 2020

Abstract: Blockchain and IoT are being deployed at a large scale in various fields including healthcare for applications such as secure storage, transactions, and process automation. IoT devices are resource-constrained, have no capability of security and self-protection, and can easily be hacked or compromised. Furthermore, Blockchain is an emerging technology with immutability features which provide secure management, authentication, and guaranteed access control to IoT devices. IoT is a cloud-based internet service in which processing and collection of user's data are accomplished remotely. Smart healthcare also requires the facility to provide the diagnosis of patients located remotely. The smart health framework faces critical issues such as data security, costs, memory, scalability, trust, and transparency between different platforms. Therefore, it is important to handle data integrity and privacy as the user's authenticity is in question due to an open internet environment. Several techniques are available that primarily focus on resolving security issues i.e., forgery, timing, denial of service and stolen smartcard attacks, etc. Blockchain technology follows the rules of absolute privacy to identify the users associated with transactions. The motivation behind the use of Blockchain in health informatics is the removal of the centralized third party, immutability, improved data sharing, enhanced security, and reduced overhead costs in distributed applications. Healthcare informatics has some specific requirements associated with the security and privacy along with the additional legal requirements. This paper presents a novel authentication and authorization framework for Blockchain-enabled IoT networks using a probabilistic model. The proposed framework makes use of random numbers in the authentication process which is further connected through joint conditional probability. Hence, it establishes a secure connection among IoT devices for further data acquisition. The proposed model is validated and evaluated through extensive simulations using the AVISPA tool and the Cooja simulator, respectively. Experimental results analyses show that the proposed framework provides robust mutual authenticity, enhanced access control, and lowers both the communication and computational overhead cost as compared to others.

Keywords: healthcare; authentication; Blockchain; information; IoT; security

1. Introduction

The Blockchain is a decentralized and distributed database system i.e., computing machines are geographically distributed [1]. Blockchain-based IoT applications (BIoT) are deployed in many areas including education, transportation, logistics, law enforcement, and health-informatics, etc. [2]. Blockchain gives the free and autonomous system, suggesting that each hub on the Blockchain structure

allows the data to be transferred, stored, and updated securely. Blockchain has demonstrated its capacity to change the conventional way of using applications to share biomedical and e-Health data [3,4]. Blockchain is a creative design for digitizing clinical history, where it is difficult to deal with the issues of records and decentralized data protection. Figure 1 shows a systematic view of the Blockchain network [5]. Data privacy and security in healthcare applications have drawn-in attention from both industry and academia. There is much literature available on the traditional security designs used as knowledge in healthcare applications. In any case, these frameworks are not appropriate to enable their prompt applications while giving security in practice for smart healthcare. Although, researchers have broadly used public-key cryptographic mechanisms, elliptic curve cryptography (ECC), bi-linear Diffie–Hellman (BDH), homomorphic encryption (HE), block cipher (BC) and ElGamal (EG) frameworks [6–11], etc. However, in all cases, there are various concerns related to these techniques i.e., public-key cryptography such as RSA depends on large integer factorization and therefore has slow processing speed. The ECC's security is based on a discrete logarithm and uses finite fields with smaller groups; however, it requires high computational cost. The EG algorithm is based on a cyclic group, and its security solely depends on the discrete logarithms and their complexities.

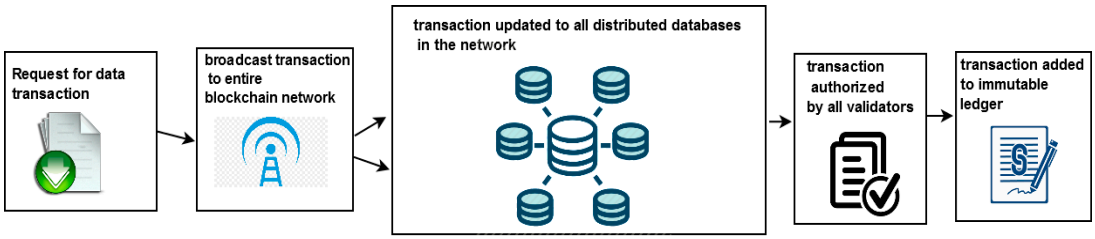

Figure 1. A comprehensive view of the Blockchain process. It is a distributed database, shared and integrated among all contenders. It ensures the integrity by encrypting, validating, and permanently recording transactions [5].

Since the introduction of the internet, it was said that it is a technology of connecting computers worldwide. But later, it has widely been used for many purposes like web browsing, file sharing, e-commerce, online banking, etc. [12,13]. The computer scientists predict and believe that the IoT holds an awesome guarantee for some lifestyle-enhancing applications [14]. The stages of such applications and operational archetypes are presented in Figure 2 [15], some other interesting architectures are also available from [16–18]. Recently, with the advent and emergence of smart technologies, the idea of ubiquitous computing came into existence i.e., IoT [18,19]. IoT has made progress in four fields, i.e., Machine-to-Machine (M2M), Internet of Vehicles (IoV), Internet of Energy (IoE), and the Internet of Sensors (IoS). M2M is a vital revolution for the realization of IoT [16]. IoT is said to be the future of the internet; a world of connected objects, therefore, it is important to use new technologies to support M2M communication [20]. Although the deployment of IoT has many influences on the smartness of human life i.e., smart intelligence, smart communities, and smart homes that would be connected through IoT [21]. Measurements of daily living activity help to indicate one's health status and judge the capabilities of living quality. So, IoT sensors can be utilized to recognize daily living activities as presented in an activity daily living (ADL) recognition system in [22]. However, it is required to make the connection more secure to protect people in the dangerous world [17,23,24]. Mutual authentication is an important factor for preserving privacy as the services will not remain safe from malicious attacks unless protection of users' personal information and other life aspects are ensured [25,26]. So, it is required to have an efficient authentication technique for fast and wide deployment of IoT devices [23,27]. Today's world has become a global village as people across the world are connected with the internet and also share data [28]. Currently, the internet is the backbone of modern knowledge and data sharing that ultimately produces large amounts of data for various services like storage, processing, analysis, and management, etc. These services are scalable, elastic, available, and reliable in terms of user needs [29,30]. IoT uses these services for processing and handling the user's data to allow

multiple operations under the umbrella which pose many issues like, privacy, integrity, authentication, and other security concerns [13,31]. Although there exist many solutions to deal with these issues, there are still various concerns to cope with [32,33].

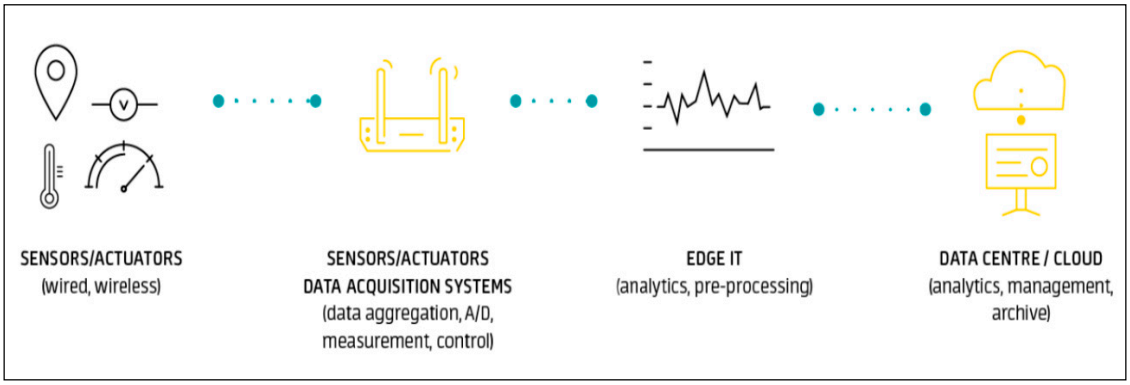

Figure 2. Applications and operational archetypal representation of the IoT network. It consists of the Things, which are objects connected to the Internet which utilizing their embedded sensors and actuators can sense the environment around them and gather the information that is then passed on to IoT gateways. The next stage consists of IoT data acquisition systems and gateways that collect the great mass of unprocessed data, convert it into digital streams, filter, and pre-process it so that it is ready for analysis. The third layer is represented by edge devices responsible for further processing and enhanced analysis of data. After that, the data are transferred to data centers which can be either cloud-based or local for further analysis [15].

Blockchain is a novel trend toward the digitization of clinical records and managing such inexhaustible information is a challenge that keeps the scientists continually active. The utilization of Blockchain for examining and aggregating individual clinical information is a potential cause of the Healthcare Data Gateway (HDG) [34]. Generally, Blockchain uses cryptography, for instance, hash limits, unequal encryption, and electronic imprints-based techniques among various collaborators in each system that helps in securing trust among them. Health informatics data sharing with security is a basic part of human administration structures to improve the quality all around social protection systems. Regardless, sharing data records among various collaborators through unbound strategies can incite spillage of the patient's records and other sensitive information. Sharing the patient's information might be separated into different health informatics systems which can incite various perils [1]. Blockchain advancement can similarly be used to store and keep up the therapeutic history of the patients. Blockchain plays an important role in keeping up the verifiable setting of records for each visit to any health center. Blockchain innovation with medicinal services information gives some security highlights [2]. The inherent characteristics of IoT result in several challenges, such as poor interoperability, decentralization, privacy, and security vulnerabilities. Blockchain technology brings opportunities in addressing the challenges of IoT through convergence of Blockchain and IoT [35]. The access control techniques manage approving clients to facilitate to authorized actions or access legitimate resources, as opposed to portraying how the client ought to be authenticated; authentication is viewed as essential for authorization. Authentication might be completed utilizing three essential accreditation classes. The primary class, "Something I am", speaks to properties about the client, including their area or biometric qualities. "Something I have" represents certifications that were given to a client; the client has the credentials. This classification incorporates a wide range of keys, tokens, cards, or even personal gadgets like cellphones. The last and most natural class is "Something I know", regularly represented by passwords, yet not restricted to them; it likewise includes the client's information on security questions, their communication history, and other data [36].

Blockchain technology is profoundly made for secure and decentralized systems administration. It can change the way the data are being stored and shared. It can likewise make the work simpler,

ensure the security and accuracy of the data, and decrease the expense of support. The data on Blockchain is immutable, which makes the information safe from alterations. Moreover, the Blockchain additionally gives information provenance that ensures the integrity of the data. All the transactions and data are stored in encrypted data blocks. The Blockchain technology has its protocols that contain the log data about the client, timestamp, and crypto-graphical data. The protocol is broadcasted over the network; it could be obvious to all the associated nodes however it is only accessible to those for which it has been created. The Blockchain-based cloud framework should take full responsibility for information transfer, processing, and or storing. When the information is on the Blockchain, any individual who approaches that Blockchain will comprehend what is new with the information. Both IoT and Blockchain technologies have their strengths and limitations. An integrated system can be proposed for health informatics to obtain their advantages at one interface. The information will be stored in the cloud to allow access from anywhere. Additionally, it will be on the Blockchain arrangement, which would make the information secure; there will be a Blockchain-based platform for the healthcare informatics to store, manage, and process the data. Several frameworks based on Blockchain have been proposed in [19,37–45] for health informatics data analysis, storage, management, and transformation. Moreover, interested readers are referred to study the review articles i.e., [46,47], that show comprehensive detailed information on the use of Blockchain in the healthcare industry.

This paper presents a lightweight authentication and authorization framework for the Blockchain-enabled IoT network to ensure the privacy and integrity of user's data. The proposed framework consists of two services i.e., applications and networks. Where, applications in IoT are cloud-based services, like public mobility assistance in which services offered seamless mobility for users to interact. The mobility is based on service management availability. In-network services, the sensed data that is to be transferred in the network which a user needs to forward into the cloud via the pre-defined path. The data are stored continuously and available all the time for each network entity such as gateway cloud services. These are designed and attached with a public-key certificate that authenticates the entire service information and data access. Experimental results analysis show that the proposed framework is robust and highly secure and reliable as compared to others.

2. Literature Review

Blockchain is a decentralized and tamper-proof database system. So, Blockchain can be used to store the medical records of patients and can also play a vital role in the field of healthcare to maintain and share medical data securely. IoT comprises billions of connected things; things could be sensors, computers, embedded devices, actuators, smartphones, etc. [37,48]. Research studies [12,49] show that traditional communication protocols such as HTTP, TCP, and IP are not efficient to support M2M communication. IEEE has launched a project to develop standards for IoT known as IEEE P2413TM [50,51]. In research articles [20,52] a three-layered architecture has been presented for IoT i.e., perception, network, and application layers. Authors of [53,54] also have proposed a three-layered architecture consisting of things, semantic and internet-oriented layers. The security problems and measures of three layers architecture are discussed in detail in [20,33,52] and summarized next: (a) perception layer: node capture, malicious node, DoS attack, timing attack, and man in the middle (MITM) attacks can occur in this layer. (b) Network layer: MITM attack, eavesdropping attack, DoS attack, replay attacks, identity authentication problems, and privacy disclosure are the main problems with this layer. (c) Application layer: data and information exposure, identity authentication, and privacy protection issues come under this category.

Authentication is one of the major issues that need to be addressed. Several authentication techniques are available in the literature to satisfy the authentication model to secure IoT i.e., mutual authentication, perfect forward secrecy, anonymity, and un-traceability, the authentication protocols use both cryptosystems and non-cryptosystems techniques [32]. These techniques are classified into four categories i.e., centralized, distributed, hierarchical, and flat. These techniques are categorized depending on the following characteristics and attributes i.e., registration phase,

two-way authentication, offline phase, additional hardware, multiple credentials, and multiple authentications. Some authentication techniques are proposed for cloud-centric IoT environment and resource-constrained devices as the two main components of IoT [20,55] as discussed subsequently. (a) Authentication in a cloud-centric IoT environment: using this authentication scheme a user's device must be registered on an authentication server. Each user is assigned a unique secret code. Unregistered devices are handled by SaaS-agent using the modified Diffie–Hellman algorithm, followed by a two-tier authentication process. In the first tier, the username and password are verified. If successful, the user is validated in the second tier by entering a predefined sequence of events on a fake server screen. Based on the above facts the authors proposed the following authentication schemes. ID-based authentication is proposed based on three roles: user, target server, and the ID provider server. ID provider calculates two hash values and sends it to the user and target server for mutual authentication. Another ID-based approach is proposed using Elliptic Curve Cryptography (ECC). An inter-cloud authentication system is proposed in which all the cloud servers are interlinked, and the user can access them using a single account. A detailed study of these techniques can be found in [33]. (b) Authentication in resource-constrained devices: in this technique, biometric-based authentication is proposed in which users register their credentials with the base station and are equipped with a smart card. The other one is the neighbor's ID-based authentication that works in a way in which the sensor is authenticated using its neighbor's ID. Moreover, an ID-based two-phase authentication technique is also proposed i.e., offline and online phase. In the offline phase, general data parameters and public keys are stored on each node and the mutual authentication is performed. A detailed study of these techniques can also be found in [33]. Moreover, a comprehensive study of attacks on M2M and defense protocols is available from [32]. The concept of Algebraic EraserTM (AE) is used to develop a public key-based algorithm that can be implemented in RFID, NFC, and IoT, etc. [56]. The AE uses the theory of braid cryptosystem for the key arrangement [57]. Although, AE claims that it had achieved high performance on lightweight devices [58,59]. But the AE mechanism requires a trusted third party to generate system parameters in the setup phase. Another public key cryptosystem NTRU is proposed in [60], which is based on polynomial algebra and probability theory. Due to moderate key size, high-level of security, and asymptotic performance, it has received more attention recently. NTRU finds optimal solutions based on the linear equation of rings, which is unlike the conventional public-key cryptosystems i.e., ElGamal, and RSA. NTRU scheme applies to lightweight devices as compared to ECC- and RSA-based solutions. One study shows that NTRU is 10 to 100 times faster than traditional public-key cryptosystem schemes [61]. However, the communication cost of NTRU is an issue in power-constrained devices, because NTRU requires the large size of both ciphertext and key. ECC is another approach uses for the development of public-key cryptosystem algorithms. ECC-based algorithms require a short key size and are suitable for IoT applications. As stated in [62–64] the 160-bit key size of ECC encryption can achieve the same security level as that of a 1024-bit RSA encryption. Various authentication protocols [59,65–68] based on ECC have been proposed for RFID research. These can be implemented for mutual authentication in IoT to achieve a high level of security. However, the scalar point multiplication of ECC algorithms is heavy for lightweight devices as compared to NTRU and AE solutions. Authors in [56] have proposed AE-based key agreement protocol (a.k.a. AAGL). They claim that the proposed protocol is lightweight and achieves high performance at low-cost platforms as compared to other public key-based systems. AE makes use of E-multiplication which is a function that cannot reveal the input from a given output. The E-multiplication function complexity linearly increases with the level of security. Therefore, it increases the efficiency of the AAGL protocol significantly. To construct the AE concept, AAGL protocol makes use of braid cryptosystem properties. In public-key cryptosystems, the braid group was introduced in [69] and later some other protocols and algorithms were also presented in [70–72]. However, some latent problems in the braid group were found as presented in [73,74]. Moreover, some other attacks are also discussed in [75–77]. Authors in [78] presented an authentication protocol for RFID known as IBIHOP. It resists against known active and passive attacks and also

secures against strong adversary attacks [79]. Although, the authors claimed that IBIHOP provides untraceable and anonymous tags to ensure security. However, the proposed protocol needs several scalar multiplications, point additions, and hash computations that consequently degrade performance. Besides, the protocol presented in [80] utilizes three cryptosystems i.e., unique information security, time-domain transformation, and spatial domain transformation. The protocol proposed in [81] utilizes two matching algorithms, specifically, correlation coefficient-based matching algorithm and deviation ratio-based matching algorithm. The aggregate message authentication codes [82] are utilized by the two methods available from [83,84]. The aggregate message authentication codes tool is a tuple of the probabilistic polynomial-time algorithms i.e., authentication, aggregation, and verification algorithms. In an IoT environment, lightweight devices communicate with each other or with the server. The bandwidth restricts low-powered devices from transmitting large messages [85]. As high efficiency is required for lightweight protocols, their computational cost should be affordable and run efficiently [86]. Open Authorization (OAuth) is a widely used authentication mechanism for IoT devices. OAuth follows token-based authentication and authorization protocol that authenticates users to access protected resources using a trusted centralized server [87–89]. The protocol consists of four factors i.e., (i) resource owner who owns and grant access to the protected resources, (ii) authorization server which issues access tokens to authorized clients, (iii) resource server which hosts the protected resources and can accept access based on tokens issued by the authentication server, and (iv) client who initiates access request. The integration of IoT with Blockchain technologies offers more robust solutions to the issues related with the interoperability, privacy, security, traceability and reliability of the system [35,90,91]. Smart contracts are the essential elements of Blockchain which enable the contractual terms of an agreement to be enforced automatically without the intervention of a trusted third party; a comprehensive review on smart contracts, their challenges and platforms is discussed in [92].

Authors of [22] presented an activity daily living (ADL) recognition framework that uses the sensor data, for example, cell phones and leads time-series sensor fusion processing. Raw data are gathered from the ADL Recorder App running on a client's smartphone with numerous embedded sensors. The core technology in this research is audio processing, positioning of indoor Wi-Fi, localization of proximity sensor, and time-series sensor data fusion. By consolidating the data of numerous sensors, the ADL Recognition System can precisely profile an individual's ADL and find life patterns. The various configurations have been applied to optimize the battery lifetime and network traffic to meet the requirement in the long run.

Authors of [41] have designed Blockchain-enabled cloud storage and sharing system for medical data. It generates a hash value of each record to store it securely. However, this system does not verify the credibility of a user e.g., someone can be registered as a patient or doctor and can store fake records repeatedly. It also does not differentiate among data formats i.e., pictures, text and or numbers as the system generates hash values and stores them. Authors of [93] developed a Blockchain-based database for sharing medical records with enhanced security. However, still there exists a chance of system failure which causes system latency i.e., if the patient consults with a different doctor of the different hospital then there is a chance of data latency. In addition, there is no reward system for the users who mine the data into ledgers. In a research paper [94], a Blockchain-based preservation system has been proposed for medical data storage and Proof of Work (PoW) protocols are being used for mining. Encryption and hashing are being used for data security and integrity. However, this model does not provide data sharing and requires high computational power and more time for mining. In a research article [43] the authors proposed a framework for storing and sharing medical records which consists of two Blockchain systems i.e., private and consortium. The analysis shows that it is better for sharing records and security. However, due to the use of two different Blockchain systems, it is very expensive and infeasible. Moreover, the proposed system does not provide any mechanism for data verification. Additionally, a comprehensive review has been presented in [95], which shows the role of Blockchain in health domains.

It is concluded that the solutions should not compromise security for achieving high performance. In this paper, we propose a lightweight authentication and authorization framework for the Blockchain-enabled IoT network in health informatics based on joint conditional probability. It generates and assigns random numbers during the distribution of data to establish a secure connection for data acquisition. The proposed framework is validated through intensive simulations. Results analysis show that the proposed framework ensures mutual authentication and provides the privacy of information.

3. Materials and Methods

In the proposed framework, a certificate authority generates certificates and keys for each user i.e., doctor, patient, and guest. All the users store the data while using the issued certificates and keys. The key is used to retrieve the data only. The user sends a certificate, key, and data to the Blockchain network. Initially, the Blockchain verifies the certificate and key, the system formats data and sends it to the interplanetary file system (IPFS). The IPFS generates a hash code of data and sends it to the Blockchain for mining using proof of authority protocol. Each minor gets reward points for mining e.g., in case, if a minor does not complete mining within the specified time interval then its rating degrades. The procedure makes use of three smart contracts i.e., (a) to check the rating of minors (b) to check the format of data and (c) to verify the user. At last, the users are equipped with a key to see profile information and other respective medical records. The proposed authentication framework makes use of the lightweight encryption protocol in sending the challenge and receiving a response to check it accordingly. The number of rounds depends on the security level and system parameters. Then authentication is performed to establish a secure channel. Several messages transfer between two nodes (i.e., sensor, server, or end-user). The process begins with sending a message along with a cipher identity credentials suit from one node to another. If the receiving node possesses the corresponding cipher identity information, then it agrees for mutual authentication or otherwise ends the communication by sending the 'end' message appended with received identity suit. In a successful authentication process, request-response messages transfer between two nodes to perform mutual authentication and establish a secure channel. This channel is then used for further data acquisitions while following the authorization rules defined in the smart contract. To perform the experiments some assumptions are taken into consideration i.e., (i) user can have one or more IoT devices, (ii) the private key is protected, (iii) user owns an Ethereum account, (iv) both the user and IoT device are connected to the Blockchain, and (v) the user will execute their own smart contract. To shape a decentralized smart contract system running on decentralized Blockchain, all the users deploy their smart contracts to achieve full control of their systems. The overall system architecture of the proposed Blockchain-enabled IoT network is presented in Figure 3.

In the proposed model, we deployed a hybrid design approach where just part of interactions and information occurs in the Blockchain and the rest are straightforwardly shared between the IoT gadgets. One of the difficulties in this methodology is selecting which interactions should experience the Blockchain and giving the best approach to choosing in real time. The integration of both technologies is an ideal solution since it uses the advantages of both Blockchain and real-time IoT connections. In this methodology, fog-computing could become possibly the most important factor to overcome the limitations of Blockchain and the IoT. In the proposed system, the IoT architecture consists of three layers i.e., physical (asset layer), communication (fog layer/gateway), and application (Blockchain integrated with cloud). The first layer contains a multi-sensor monitoring network that assesses the patient's dynamic readings like medical intakes, and physical actions, to analyze it and determine conditions. The second layer consists of fog devices that collect the information gathered by the sensors, translate it into meaningful data streams, and transfer it to a back-end destination. The third layer is where data are received, stored, and processed using cloud-based data analysis engines and machine learning algorithms integrated with Blockchain. The resulting instincts can be used to advise the proper healthcare service or applied in further research. For the validity of transactions in the

Blockchain, Ethereum Solidity is used to execute PoW smart contracts. The reason behind using PoW is the decentralized platform and adaptation of the account-based model.

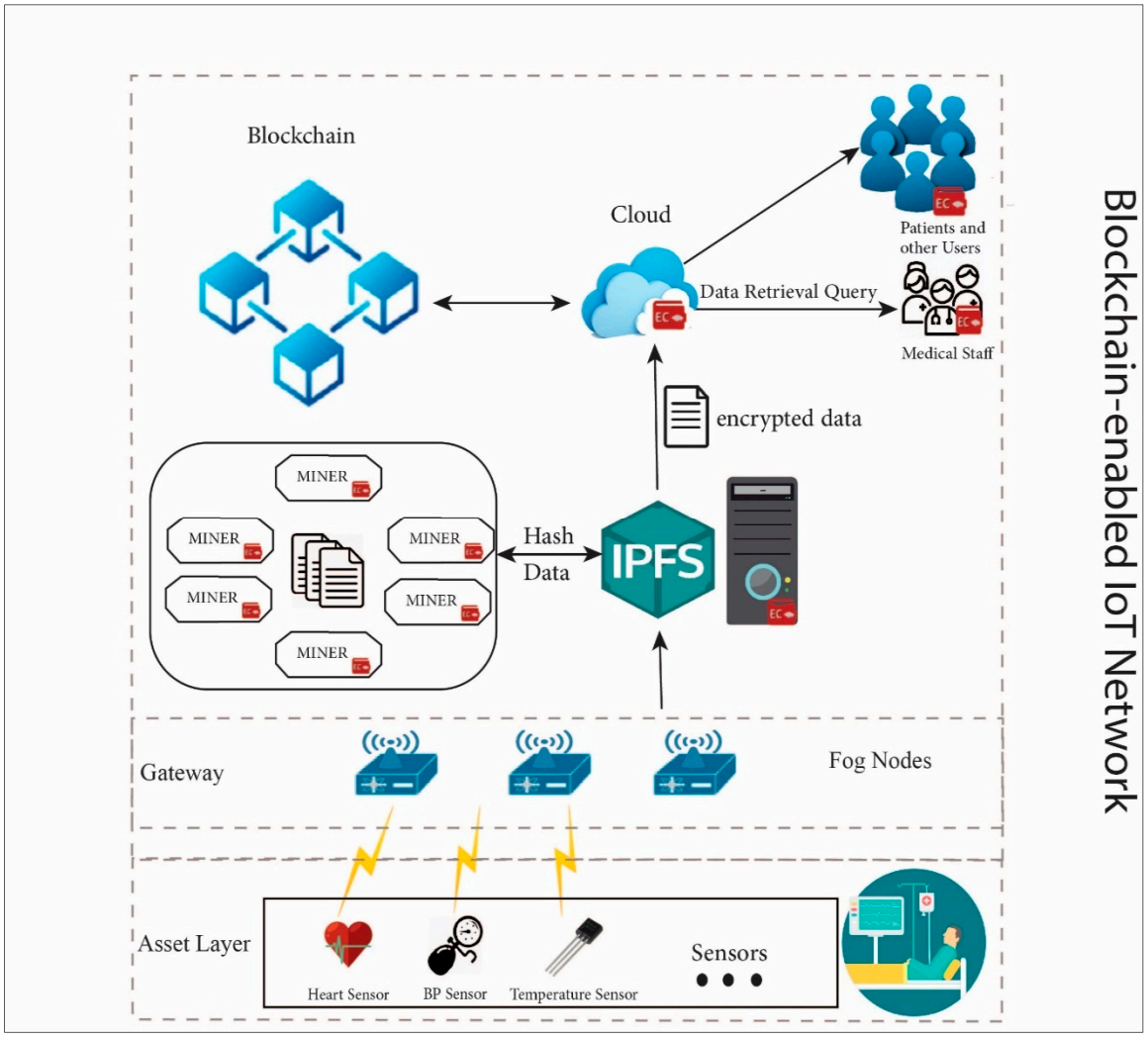

Figure 3. The overall system architecture of the proposed Blockchain-enabled IoT network. It consists of three layers i.e., physical layer (assets), communication layer (gateway), and application layer (Blockchain integrated with cloud).

3.1. Random Number Generation

This section describes the generation of random numbers used in the authentication process of IoT devices. Suppose that IoT devices are denoted as $d_1, d_2, d_3 \ldots d_n$, where n is the number of devices. Each IoT device d has assigned a real number $r(d_i)$ for correspondence, where $0 < i \leq m$. Now, random numbers $r_1, r_2, r_3 \ldots r_n$ are generated as authentication values. The function $r(.)$ is used to match IoT devices with corresponding real numbers. Joint conditional probability $P_{xy}(x_j,y_j)$ is calculated for given two random variables x and y to authenticate IoT devices when $x = x_j$ and $y = y_j$. If x and y are matched, then they will become mutually authenticated. This process has two cases as presented next.

3.1.1. Homogenous IoT Devices

In the case of homogeneous IoT devices mutual authentication, the probability is calculated as given in Equations (1) and (2).

$$P_{xy}(x_i,\ y_i) = P_x\left(x_j\right)P_y\left(y_j\right) \quad (1)$$

$$P_{xy}(1,1) = P_{xy}(1-1) = P_{xy}(-1,1) = P_{xy}(-1,-1) = \frac{1}{4} \tag{2}$$

Generally if x and y are n-series (i.e., n = 1, 2, 3, … n) then Equation (3) exist as:

$$\sum_i \sum_j P_{xy}\left(x_j, y_j\right) = 1 \tag{3}$$

3.1.2. Heterogeneous IoT Devices

In the case of heterogeneous IoT devices authentication, the joint conditional probability for x and y will be as shown in Equation (4).

$$\sum\nolimits_i P_{x|y}(x_i|y_i) = \sum\nolimits_j P_{y|x}\left(y_j|x_j\right) = 1 \tag{4}$$

So, $\sum_i P_{x|y}(x_i|y_i)$ shows the probability for each union, where condition $y = y_i$ holds. This process can also be applied to its joint event j i.e., $\sum_j P_{y|x}(y_j|x_i)$ that generates Equation (5) and leads to Equation (6) as given next.

$$P(X \cap Y) = P(X)P(Y|X) \tag{5}$$

$$P_{x|y}\left(x_i|y_j\right) = \sum\nolimits_i P_{x|y}\left(x_i|y_j\right) = \sum\nolimits_j P_{y|x}(y_j|x_i) \tag{6}$$

The heterogeneous devices and platforms may generate the probability as shown in Equation (7).

$$\sum\nolimits_i P_{xy}\left(x_i, y_j\right) = \sum\nolimits_i P_{x|y}\left(x_i|y_j\right)P_y\left(y_j\right) = P_y\left(y_j\right) \sum\nolimits_i P_{x|y}(x_i|y_i) = P_y\left(y_j\right) \tag{7}$$

Similarly, Equation (8) is used to guarantee the authentication of heterogeneous IoT devices.

$$P_x(x_i) = \sum\nolimits_j P_{xy}\left(x_i, y_j\right) \tag{8}$$

When IoT devices perform authentication, both Equations (7) and (8) are used for recognizing heterogeneous IoT devices in various environments via the fractional probabilities $P_x(x_i)$ & $P_y(y_j)$ of the authentication information embedded in the smart contract.

3.2. Proposed Authentication Framework

It is assumed that the keys are generated and assigned to each participant in the Blockchain-enabled IoT network. It is also assumed that the authorized user has also stored information on the devices. Two IoT devices X and Y perform mutual authentication as follows. X randomly selects a number R_{nx} from a pool bounded as $0 \leq R_{nx,1} \leq log(id_{max}/2)$ where id_{max} is the length of identity number in bits. The selected number along with the message is encrypted using $Y's$ public key and forwards to Y as described below.

$$Step\ 1: \ X \rightarrow Y: \ \vartheta_a = E\left(PuK_y(X, R_{nx}, 1)\right)$$

The message ϑ_a receives at Y and decrypts to get the intended message.

$$Step\ 2: \ \varepsilon_{a,1}, R_{nx,1} \leftarrow DE_{PrKy}(\vartheta_a)$$

Here, the comparison is performed for mutual authentication. Upon the success of equality, Y chooses a number randomly R_{ny} bounded by $0 \leq R_{ny} \leq id_{max}/2$ and responds as

$$Step\ 3: \ \vartheta_b = E(PuK_x\left(R_{ny,1}, Y \times R_{nx}\right)$$

X receives the response from Y and decrypts it as

$$Step\ 4: R_{ny}, \varepsilon_y \leftarrow DE_{PrKx}(\vartheta_b)$$

The acceptance is subjected to equality of ε_y and $Y \times R_{nx}$. If accepted, then X computes the response and sends it to Y.

$$Step\ 5: \ \vartheta_c = E\Big(PuK_y\Big(X, R_{ny,1}, R_{nx,2}\Big)\Big)$$

where $R_{nx,2}$ is bounded by $0 \leq R_{nx} \leq id_{max}/2$. X and Y communicate via challenge and response messages until $(n-1)th$ message exchanges. When X receives $(n-1)th$ message it decrypts and obtains information as follows.

$$Step\ 6: (R_{nx,z}, \varepsilon_{y,z}) \leftarrow DE_{PrKx}\ (\vartheta(n-1))$$

If $\varepsilon_{y,z} = Y \times R_{nx,z}$, So, X calculates response ϑ_n and sends to Y as

$$Step\ 7: \ \vartheta_n = E\Big(PuK_y(X, R_{nx}, z, 0)\Big)$$

Y decrypts the message and obtains information as

$$Step\ 8: \ (\varepsilon_{x,z+1}, \tau) \leftarrow \ DE_{PrKy}(\vartheta_n)$$

Then checks for

$$Step\ 9: (\varepsilon_{x,z+1}) = \Big(X, R_{ny,z}\Big)\ \&\ \tau = 0$$

If the above conditions hold then the corresponding devices are mutually authenticated successfully, or have otherwise failed. The proposed framework takes n-passes in the mutual authentication process. The value of n is dependent on system parameters and the security level of the encryption algorithm. Notably, the 64-bit security level is desired for the proposed framework. Then X and Y randomly selects numbers R_{nx} and R_{ny} related as $logR_{nx} = logR_{ny} = 64$. These processes will take 3 passes for mutual authentication of corresponding devices.

3.3. Experimental Setup

All the experiments are performed on Intel(R) Core i5 Dell Optiplex-3050 with four core CPUs@3.4 GHz, 16-GB of memory installed, running on 64-bit instruction set kernel Linux (Ubuntu 16.04 LTS) OS. Two android smartphones and a laptop are used as clients. Open source Contiki 2.7 OS and Cooja simulator are used for authentication and emulation of IoT devices. The default configurations of sky mote in Contiki were considered for implementation. AVISPA tool has been utilized to check the validity of the proposed algorithm [96]. Truffle Ganache framework and Meta-Mask connected with web3 interface are used for simulation of Blockchain-enabled IoT network, where SolMet-solidity parser [97] is used for evaluation and analysis of smart contracts. The proposed and competitive protocols are implemented in the Cooja simulator along with sky motes for evaluations. We compare the proposed framework with state of the art authentication protocols i.e., RSA, X.509, and with some other known protocols i.e., multi-tier authentication [98], ID-based authentication [99], and lightweight security solution [100] for a fair comparison. Security protocols implemented on the lower layer do not guarantee E2E communication security. In the application level, the Datagram Transport-Level Security (DTLS) is widely used in IoT. Some ECC-based variants of DTLS are also used with X.509 and RSA. The key drawback of RSA is large-sized key (i.e., 2048) and of the X.509 standard is certificates have 1 kb size which is inadequate for IoT devices. We evaluated all the experiments on common and critical parameters i.e., mutual authentication robustness, security strength, communication, and computational overhead. The smart contracts are analyzed on standard parameters listed in Table 1. The Cooja simulator configuration is presented in Table 2. The read latency ℓr, read throughput T_r, transaction latency ℓ_t, and transaction throughput T_t are computed using Equations (9)–(12), respectively.

$$l_r = response^{time} - submission^{time} \tag{9}$$

$$T_r = \frac{read\_operations^{total}}{total\_time^{seconds}} \tag{10}$$

$$\ell_{\mathrm{t}} = confirmation^{time} - submission^{time} \tag{11}$$

$$T_{\mathrm{t}} = \frac{total\_transactions^{committed}}{total\_time^{seconds}} \tag{12}$$

Table 1. Measurement parameters used for the analysis of smart contracts.

S.No	Parameter	Descriptions
1.	SLOC	Source lines of code
2.	LLOC	Logical lines of code
3.	NF	Number of functions
4.	NL	Nesting level
5.	NLE	Nesting level else if
6.	NUMPAR	Number of parameters
7.	DIT	Depth of inheritance tree
8.	NOA	Number of ancestors
9.	NOD	Number of descendants
10.	NA	Number of attributes (i.e., states)
11.	Read Latency	The time interval between reading request and response
12.	Read Throughput	Measurement of read operations completed in a defined timeframe
13.	Transaction Latency	The time from the submission of a transaction until the generation of results in the network
14.	Transaction Throughput	The frequency of transactions submission over the Blockchain network.

Table 2. Cooja simulator parameter configuration.

S. No	Parameter	Configuration
1.	Radio Medium	Unit Disk Graph Medium (UDGM)
2.	Mote Startup Delays	1000 ms
3.	Random Speed	123,456
4.	New Random seed on reload	ON
5.	Simulation area	550 m × 550 m
6.	Number of thresholds	Fixed i.e., 3000, 6000, 12,000, 24,000, 48,000
7.	Number of IoT devices	15, 30, 60, 120 and 10, 35, 75, 100 and Random
8.	Data generation interval	0.1 ms
9.	Transmission of IoT device	25 m
10.	Initial dataset time	2.0 h

4. Results and Discussion

The general IoT healthcare model comprises of a device, cloud, and client layers. The device layer comprises of several internet-enabled sensor nodes. Data acquisition and communication protocols are used to send the data to storage for further analytics. These devices permit the client to gather data continuously with various frequencies. The cloud layer, that has the information gathered from the sensors for further processing i.e., features extraction etc. This data then fed into a decision support system to provide a decision regarding the health of a concerned person. The client layer comprises of the receiving user and can be in a different form, of concern is the smart devices. Security and privacy of users' data is the big challenge to deal with. Therefore, within the limits of three layers, a module Blockchain for instance can be added to ensure the reliability of the healthcare system. Blockchain technology can cope with the major issues experienced in healthcare from the perspective of information exchange. With today's e-health systems, error rates for identifying records are as high as 25% for healthcare organizations, and higher even i.e., 50 to 60 percent outside of these systems. Blockchain technology can provide solutions to these challenges: (a) patients can become more engaged with their health if they can gain access to cryptographically secure, irreversible, and immutable historical and real-time data. More importantly, health professionals' quick access to this data can significantly improve the response rate to their respective situations. (b) The use of identity management in P2P

networks can give patients the ability to share their healthcare data to support medical research and innovations. (c) Important genomic and user-generated data, especially data generated by new technologies like health apps and IoT-supported healthcare devices and wearable computers can be captured and stored securely. (d) The Blockchain network would supersede the previous systems that prevented data exchange among different healthcare systems, and at the same time, reduce the costs and difficulty of data reconciliation among them.

In practice, all the information from clinical gadgets, labs, and numerous different sources are solidified and raw data is produced at a large scale called big data. These data are the fundamental elements of the entire Blockchain-based healthcare framework, and are the foremost segment that makes the main layer of the stack. Blockchain technology resides on the top of the raw data layer that is viewed as the core structure in interest to build a secure health informatics framework. Each Blockchain framework has various features, for example, protocols and consensus algorithms. Blockchain encourages clients to make and deal with transactions. A few Blockchain systems exist and are being used, for example, Ethereum, Ripple, and Hyperledger Fabric. The essential part of the Blockchain is a smart contract. The existence pattern and life cycle of a smart contract comprise four significant stages i.e., creation, deployment, execution, and completion. For communications with other frameworks or across various systems, a wide scope of protocols could be utilized. For instance, this may include P2P, distributed, centralized, and decentralized. When the platform is made by actualizing Blockchain technology, the next phase is to guarantee that the applications are incorporated with the entire framework. Blockchain-based health informatics applications can be classified into three wide classes i.e., data management, SCM applications, and IoMT. IoMT includes integration of healthcare IoT and clinical gadgets, healthcare IoT framework, and data security. However, the stakeholder layer resides at the top of hierarchical structure, which comprises of the individuals and parties who take advantage of the Blockchain-based health frameworks i.e., doctors, patients, and other users. The principal concern of all the stakeholders at this layer is to successfully share, process, and manage information without risking its security and protection.

The frequencies of the individual metric values are computed for both user and migration Solidity smart contracts. In Table 3, the migration Solidity smart contract metric value for NF shows the number of functions in which most contracts contain 1 to 10 value, and the value above 30 is very rare. NL and NLE are 0 or 0.5 which shows that the control structures are not nested into each other. It is observed that the tendency for nesting level is the same for all the smart contracts. A variety of contracts are falling in 0 and 1 level, so it is noted that the nesting level plays an important role in smart contracts code for Solidity. The same tendency is observed for the nesting level in other smart contracts. Most of the contracts have an average nesting level between 0 and 1, indicating that deeply nesting control structures are very uncommon in Solidity smart contracts. The metric values for user Solidity smart contract show that the majority of contracts contain 0 to 14 functions and an NF value above 5 is very rare, NL, NLE, DIT, NOA, and NA are 0 or 0.5 which means that the control structures are indeed not nested deeply into each other. It is observed that the tendency for nesting level is almost the same as depicted in migration Solidity smart contracts. Most of the smart contracts are falling in between level 0 and 1. The NUMPER, LLOC, and NF show that most smart contracts contain 1 to 1100 functions. Results analysis shows that the nesting level of smart contracts is critical and very important.

Read latency is the time required to fetch results and display them on the application interface. For analysis, initially, the read latency for 100 transactions is recorded and then extrapolated to 500 transactions. Figures 4 and 5 show the read latency and read throughput analysis for 500 transactions, respectively. The trend in the graph shows that the number of transactions increases with time in seconds. With the increase in the number of transactions, the time required to read data from each block also increases, and hence it generates the linear curve. The throughput of the proposed model for Blockchain depends on the number of transactions. In the analysis of the results, it is observed that as the number of transactions increases, the throughput of the system also increases.

Table 3. Comparative analysis of smart contract parameters in Blockchain.

Parameters	Migration Solidity Metric Value	User Solidity Metric Value
SLOC	13	140
LLOC	5	80
NF	3	2
NL	0	1
NLE	0	0
NUMPER	1	12
DIT	0	1
NOA	0	1
NOD	3	0
NA	0	5

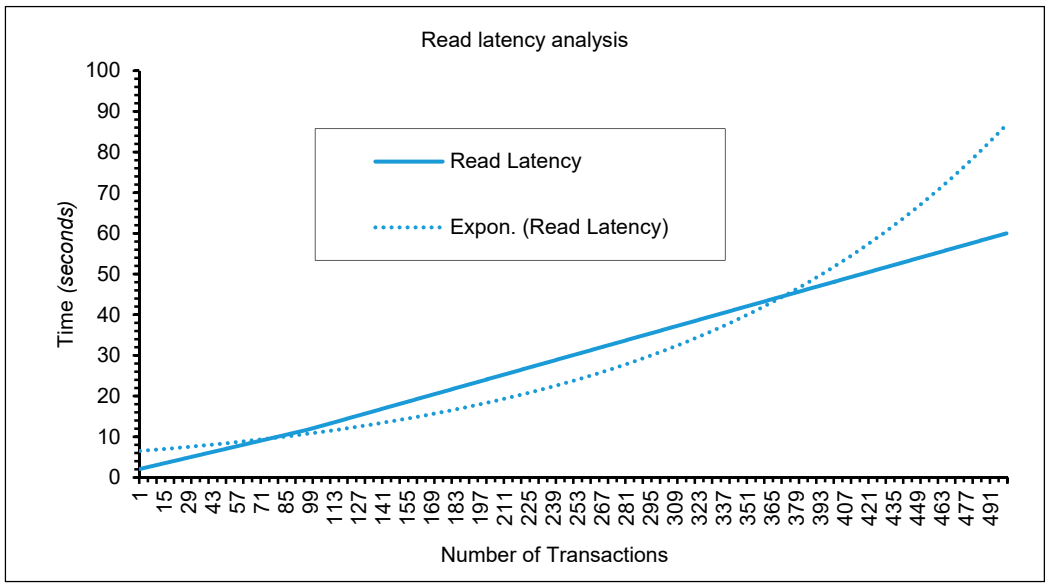

Figure 4. Read latency analysis for 500 transactions in the Blockchain.

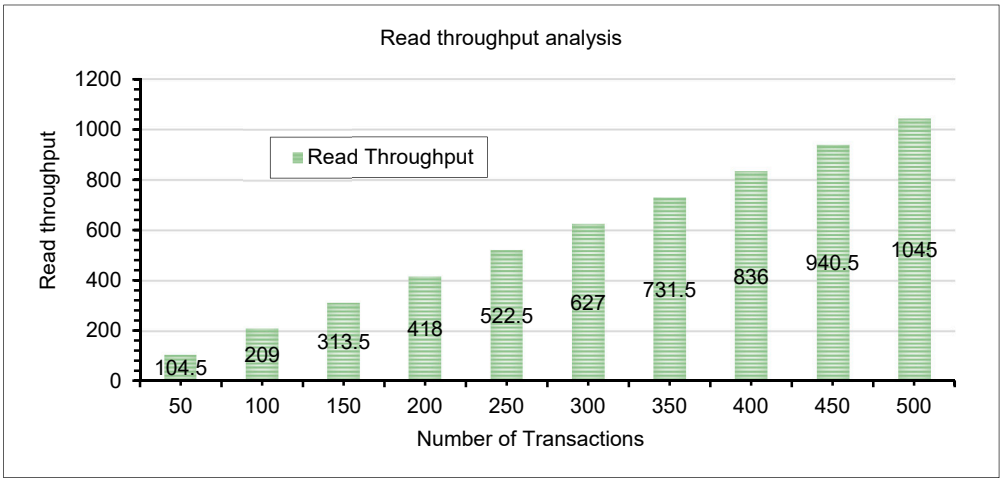

Figure 5. Read throughput analysis for 500 transactions in the Blockchain.

Transaction latency is the time required to confirm a transaction. It can be calculated by subtracting the confirmation time from the submission time. Transaction latency depends on the size of a transaction. Moreover, an increase in the size of a transaction consumes more power and hence causes more latency. Figures 6 and 7 present results for transaction latency and throughput analysis for 500 transactions,

respectively. Transaction latency depends on the transaction size. It is clear from the figure that the throughput of the system increases with the time, which means that the throughput of the proposed model for Blockchain depends on the number of transactions and frequency.

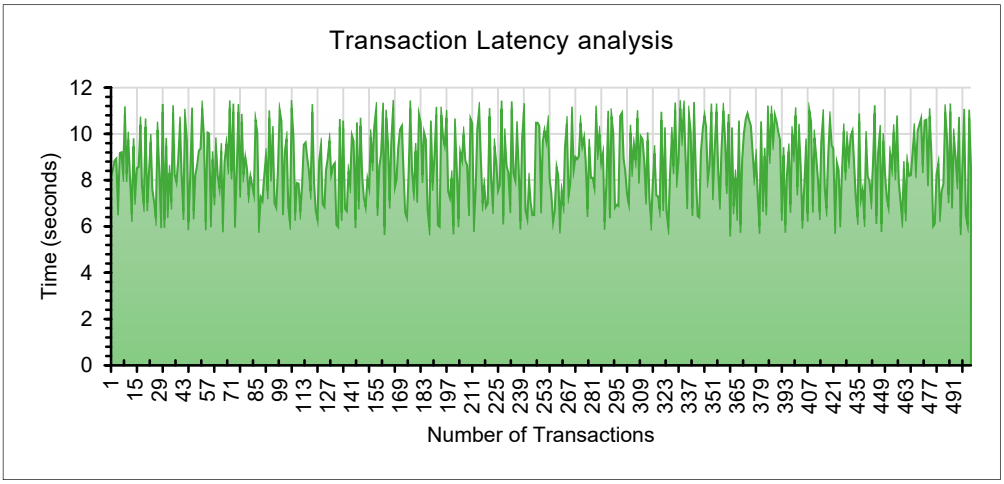

Figure 6. Transaction latency analysis for 500 transactions in the Blockchain.

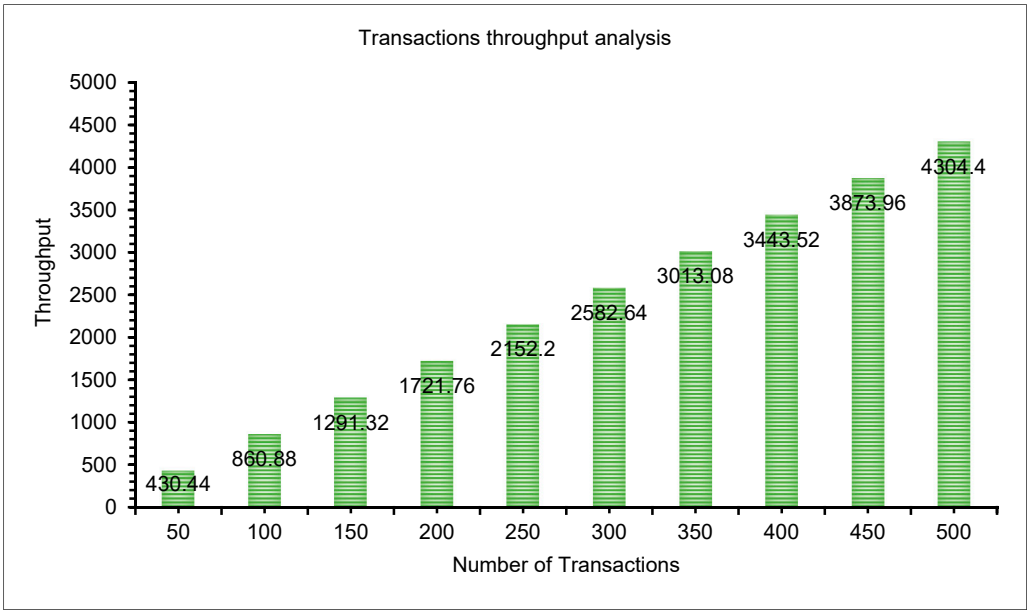

Figure 7. Throughput analysis for 500 transactions in the Blockchain.

4.1. Mutual Authentication Robustness

It is assumed that the corresponding keys and respective mote identities are pre-configured securely. Suppose that the selected random number (R_n) is m bits. So, $(R_n - 1)m/2$ bits is the level of security. The proposed mutual authentication framework relies and is based on the encryption approach. Mutual authentication between devices takes place using random numbers as discussed above. Therefore, if an eavesdropper desires to forge a valid device then it is required to generate valid messages. However, due to having no information about random numbers the eavesdropper cannot generate valid messages. The results analysis shows that the proposed encryption scheme is more secure than others. Moreover, it also resists against impersonation and MITM attacks.

4.2. Security Strength

The healthcare frameworks are beset with challenges in assuring its users of the authenticity to provide integrity and privacy to their data. Blockchain technology can be used to benefit healthcare systems. For instance, the AVISPA tool is used for algorithm validation and evaluation of security strength. The results evaluation regarding security strength between IoT devices shows that information is exchanged securely. As a result, the proposed framework shows a 6.3% improved efficiency as compared to others. It is also observed that the proposed framework has improved the strength of security regardless of the number of IoT devices. Figures 8–10 show the security strength of compromised IoT devices in balanced increasing order, imbalanced increasing order, and random order, respectively. If an eavesdropper aims to impersonate the legitimate device using a message, the associated device (i.e., access point, router) will reject the authentication request as it only accepts the random number-based calculated value, which is known to legitimate devices only. Results analysis shows that the proposed algorithm is more secure than others as their ratios are a bit higher.

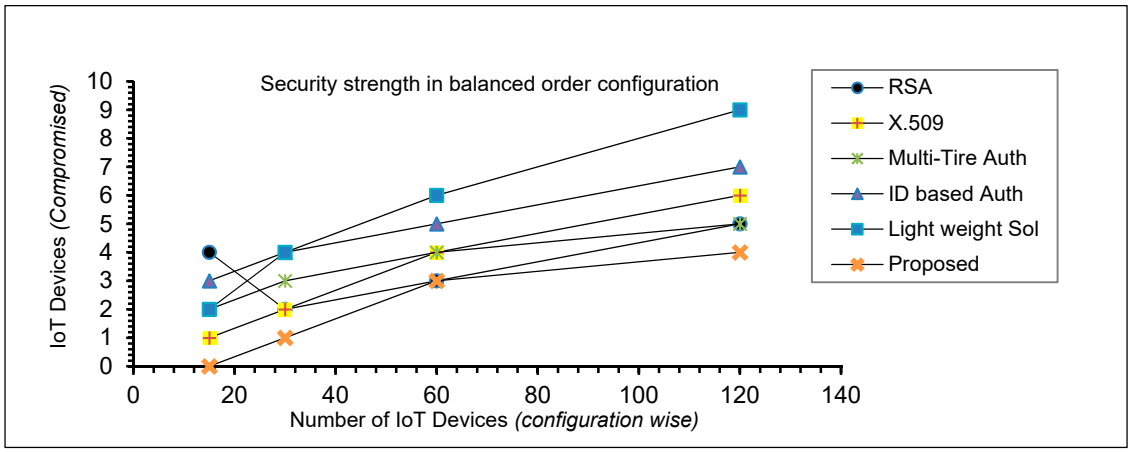

Figure 8. Compromised IoT devices security strength in a balanced order.

4.3. Communication Overhead

A small overhead has been observed in the authentication process due to the interactions. On average, overheads are lowered by 3.8% in IoT devices as compared to others. So, it has increased the information transformation. However, the overhead is due to random variable selection and mutual messages exchange for authentication, which cannot be ignored. Figure 11 shows the overhead cost observed, the plot shows the relation of time consumed in milliseconds and data processed in kilobytes. The network and bandwidth requirements for IoT networks can be optimized to increase QoS to provide instant response to the queries in life-saving applications in critical situations.

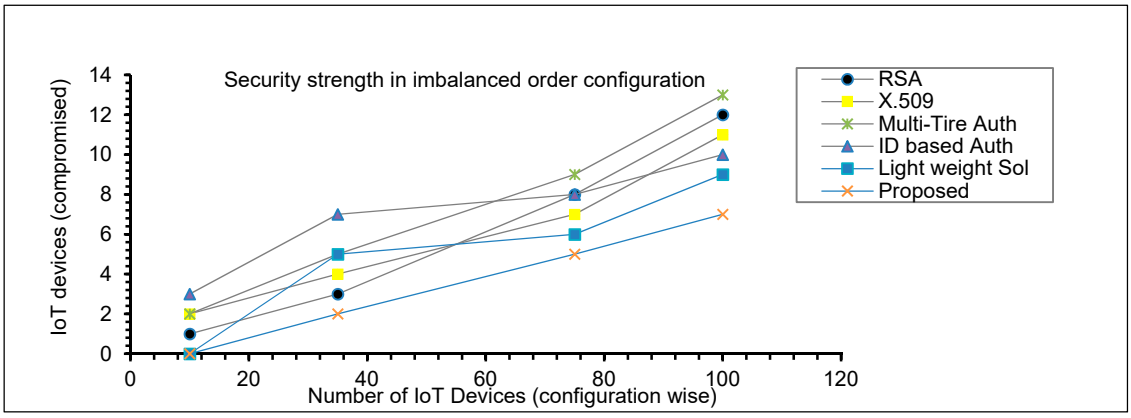

Figure 9. Compromised IoT devices' security strength in imbalanced order.

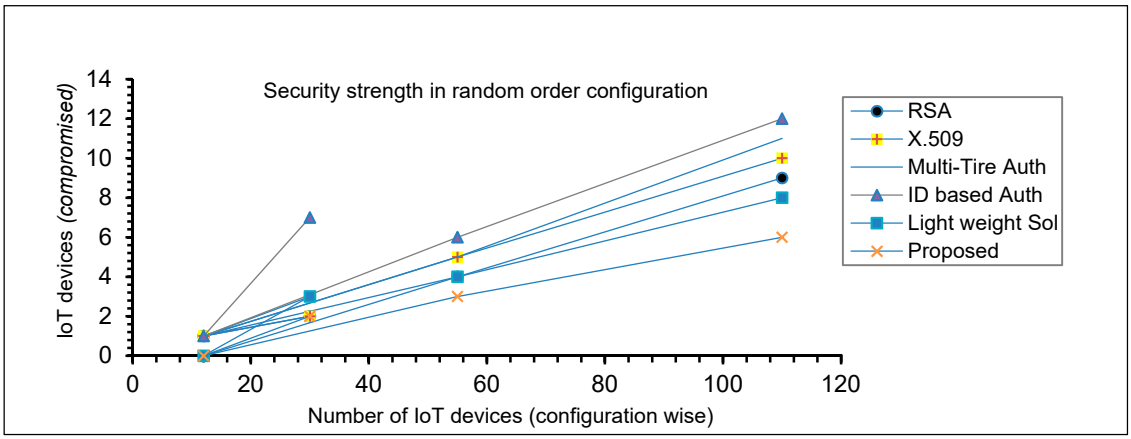

Figure 10. Compromised IoT devices' security strength in a random order.

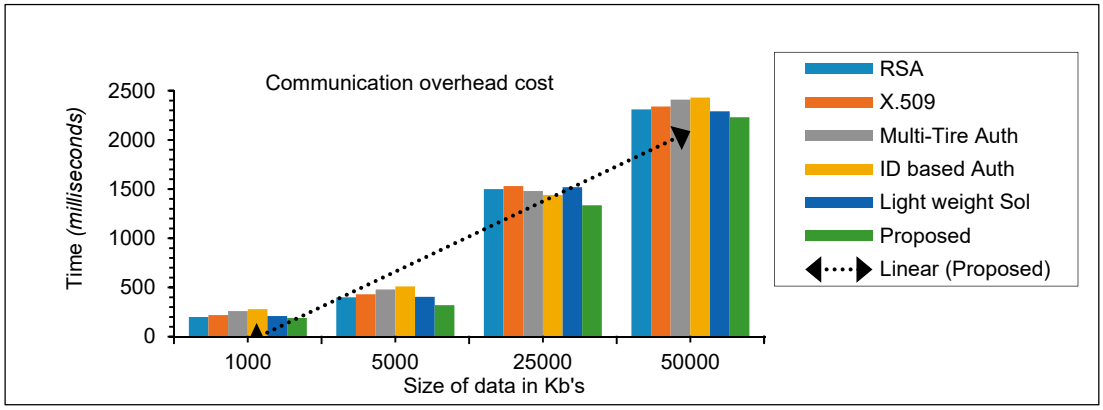

Figure 11. Communication overhead cost comparison in the data processing.

4.4. Computational Overhead

Results analysis shows that the computational cost is lessened by approximately 5.2% on average as compared to existing frameworks. However, in some cases, no differences were observed. The observation shows that this random behavior resulted due to the use of random variables and distributed joint conditional probability computation from data available. Results analysis also shows that the proposed framework does not provide indistinguishability in the case of the ciphertext chosen. IoT devices require light computation to attain desired and required security levels. Therefore, the proposed IoT authentication framework provides a lightweight mechanism of computation, which saves computational time. Figure 12 shows the comparison of data process time in Blockchain-enabled IoT devices. Its analysis shows that the proposed framework takes less time in all cases as compared to others.

4.5. Resistance against Attacks

Experimental analysis of the AVISPA tool shows that the proposed authentication framework is more resilient to adversary attacks i.e., impersonation and MITM attacks. Moreover, the proposed framework has a low communication overhead and computational cost. It can easily be implemented in the real physical hardware environment of the IoT network. It is also concluded that the proposed framework is highly secure against a malicious adversary in a random model. The proposed framework is evaluated against a MITM attack, timing attack, insider attack, replay attack, impersonation attack, password guessing attack, forgery attack, eavesdropping attack, and DoS attack. Table 4 shows the comparative results of security attacks. The table presents that either an algorithm resists against a specific attack or not. The proposed framework is based on distributed joint probability and selection

of random variables from available data. The process uses scalar point multiplication, which ensures security under the random model. It is known that DoS attacks can be launched against IoT. So, the proposed authentication phase uses robust certificates for the exchange of cryptographic credentials that avoids DoS attacks. To keep and maintain message freshness during handshake, the cryptographic random number is used. Moreover, the proposed authentication framework supports edge devices' mobility and new code addition.

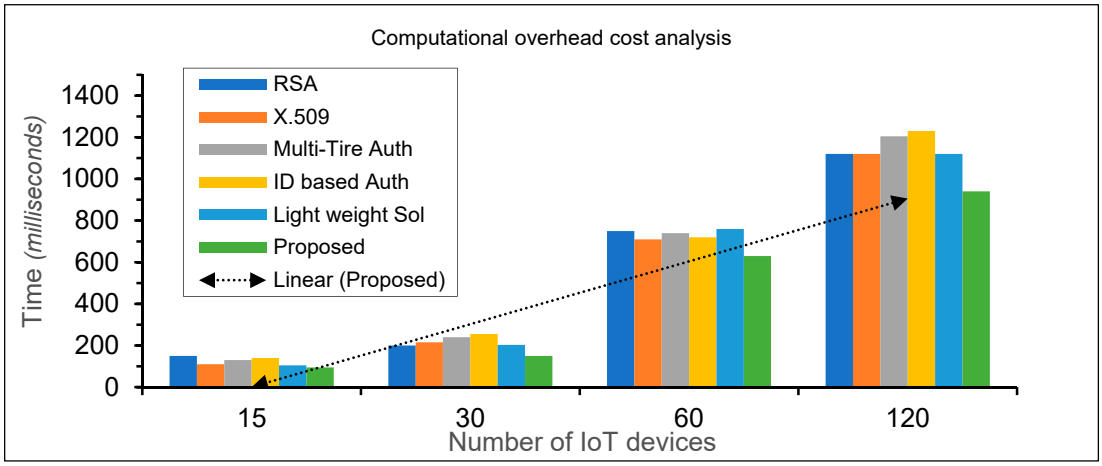

Figure 12. Computational overhead cost comparison.

Table 4. Comparative results of the proposed framework with existing schemes.

Attacks	RSA	X.509	Multi-Tire Auth	ID-Based Auth	Lightweight Sol	Proposed
DoS	Yes	No	Yes	No	No	**Yes**
Eavesdropping	Yes	Yes	No	Yes	No	No
Forgery	Yes	No	Yes	No	Yes	**Yes**
Impersonation	Yes	Yes	No	Yes	Yes	**Yes**
Insider	No	No	Yes	No	Yes	No
Man-in-middle	Yes	Yes	Yes	Yes	Yes	**Yes**
Replay	Yes	Yes	Yes	No	No	**Yes**
Timing	No	Yes	No	Yes	No	**Yes**

4.6. No Clock Synchronization and Independence of Session Key

In the proposed framework, it is not necessary to synchronize the clock of the IoT gadgets e.g., authentication server, smart sensor, and router, etc. as the messages are exchanged between the devices are similar to the messages exchanged in the nonce-based authentication method which does not depend on timestamps. In case an eavesdropper compromised the session key, the router and smart sensor can generate a new session key. It is possible due to the random number-based session key generation and independence of the prior session key.

5. Conclusions

Currently, IoT and Blockchain are the fertile areas of promising research in various fields including healthcare. Healthcare integrated with IoT has become one of the most emerging areas in Blockchain research. A large amount of data that are managed by the health sector needs to be processed steadily. It is a growing trend toward the digitization of clinical records. In the future, the smart contract can be utilized in numerous fields of Blockchain to achieve optimal performance. An extensive research consideration has been performed on Blockchain-based applications for managing the ledger, specifically in the health domain.

Although recent advancements in IoT are promising in terms of rewards, still many things need to be improved. So, companies are making challenging decisions in Blockchain- and IoT-based projects.

The diversification of IoT products and the Blockchain environment poses many challenges like authentication, privacy, chaos, mining, and management, etc. Mutual authentication is an important aspect of IoT applications because it provides security to users and guarantees authenticity and ensures the privacy of data. Based on the authentication and evaluation models, mutual authentication of IoT devices has been divided into different classes. In this paper, we address the authentication and authorization issue and present a novel solution for mutual authenticity and authorization. The proposed framework is based on distributed joint conditional probability integrated with the selection of the random numbers, which ensures the robustness. The performance evaluation and results analysis show that the proposed framework achieves more security strength, less communication overhead costs, and takes less time in processing data along with improved security. In the future, we plan to evaluate the proposed framework on hardware in a realistic environment. Moreover, the proposed framework could also be modified by applying a different consensus algorithm to make it more efficient.

Author Contributions: Conceptualization, M.T. and M.S.; methodology, M.T., M.S. and M.S.K.; software, M.T., M.S., and M.S.K.; validation, M.S., S.M., and M.S.K.; formal analysis, M.T., and S.M.; investigation, M.T., M.S., S.M., and M.S.K.; resources, M.T., and M.S.; data curation, M.T., M.S.K., and S.M.; writing—original draft preparation, M.T., and M.S.; writing—review and editing, M.S., S.M., and M.S.K.; visualization, M.T., M.S., and M.S.K.; supervision, M.T.; project administration, M.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: All the authors are grateful to those who provide guidelines and suggestions throughout this research work.

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

References

1. Udokwu, C.; Kormiltsyn, A.; Thangalimodzi, K.; Norta, A. The state of the art for blockchain-enabled smart-contract applications in the organization. In Proceedings of the 2018 Ivannikov Ispras Open Conference (ISPRAS), Tokyo, Japan, 22–23 November 2018; pp. 137–144.
2. Bennett, B. Blockchain HIE Overview: A Framework for Healthcare Interoperability. *Telehealth Med. Today* **2017**, *2*, 1–6. [CrossRef]
3. Casino, F.; Patsakis, C.; Batista, E.; Borràs, F.; Martínez-Ballesté, A. Healthy routes in the smart city: A context-aware mobile recommender. *IEEE Softw.* **2017**, *34*, 42–47. [CrossRef]
4. Zheng, Z.; Xie, S.; Dai, H.-N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
5. Siyal, A.A.; Junejo, A.Z.; Zawish, M.; Ahmed, K.; Khalil, A.; Soursou, G. Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. *Cryptography* **2019**, *3*, 3. [CrossRef]
6. Yang, Y.; Zheng, X.; Tang, C. Lightweight distributed secure data management system for health internet of things. *J. Netw. Comput. Appl.* **2017**, *89*, 26–37. [CrossRef]
7. Patranabis, S.; Shrivastava, Y.; Mukhopadhyay, D. Provably secure key-aggregate cryptosystems with broadcast aggregate keys for online data sharing on the cloud. *IEEE Trans. Comput.* **2017**, *66*, 891–904. [CrossRef]
8. Huang, H.; Gong, T.; Ye, N.; Wang, R.; Dou, Y. Private and secured medical data transmission and analysis for wireless sensing healthcare system. *IEEE Trans. Ind. Inform.* **2017**, *13*, 1227–1237. [CrossRef]
9. Ara, A.; Al-Rodhaan, M.; Tian, Y.; Al-Dhelaan, A. A secure privacy-preserving data aggregation scheme based on bilinear ElGamal cryptosystem for remote health monitoring systems. *IEEE Access* **2017**, *5*, 12601–12617. [CrossRef]
10. Gope, P.; Hwang, T. BSN-Care: A secure IoT-based modern healthcare system using body sensor network. *IEEE Sens. J.* **2016**, *16*, 1368–1376. [CrossRef]
11. Li, M.; Yu, S.; Zheng, Y.; Ren, K.; Lou, W. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *IEEE Trans. Parallel Distrib. Syst.* **2013**, *24*, 131–143. [CrossRef]
12. Li, S.; Da Xu, L.; Zhao, S. The internet of things: A survey. *Inf. Syst. Front.* **2015**, *17*, 243–259. [CrossRef]

13. Khan, R.; Khan, S.U.; Zaheer, R.; Khan, S. Future internet: The internet of things architecture, possible applications and key challenges. In Proceedings of the 10th International Conference on Frontiers of Information Technology, Islamabad, Pakistan, 17–19 December 2012; pp. 257–260.
14. Sardaraz, M.; Tahir, M. A Hybrid Algorithm for Scheduling Scientific Workflows in Cloud Computing. *IEEE Access* **2019**, *7*, 186137–186146. [CrossRef]
15. AVSystem. Available online: https://www.avsystem.com/blog/what-is-iot-architecture/ (accessed on 13 June 2020).
16. Aijaz, A.; Aghvami, A.H. Cognitive machine-to-machine communications for Internet-of-Things: A protocol stack perspective. *IEEE Internet Things J.* **2015**, *2*, 103–112. [CrossRef]
17. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Gener. Comput. Syst.* **2013**, *29*, 1645–1660. [CrossRef]
18. Zheng, L.; Chen, S.; Xiang, S.; Hu, Y. Research of architecture and application of Internet of Things for smart grid. In Proceedings of the 2012 International Conference on Computer Science and Service System, Nanjing, China, 11–13 August 2012; pp. 938–941.
19. Rubí, J.N.S.; Gondim, P.R.d.L. Interoperable Internet of Medical Things platform for e-Health applications. *Int. J. Distrib. Sens. Netw.* **2020**. [CrossRef]
20. Ma, Z.; Shang, X.; Fu, X.; Luo, F. The architecture and key technologies of Internet of Things in logistics. In Proceedings of the International Conference on Cyberspace Technology, Beijing, China, 23 November 2013; pp. 464–468.
21. Schulz, P.; Matthe, M.; Klessig, H.; Simsek, M.; Fettweis, G.; Ansari, J.; Ashraf, S.A.; Almeroth, B.; Voigt, J.; Riedel, I. Latency critical iot applications in 5g: Perspective on the design of radio interface and network architecture. *IEEE Commun. Mag.* **2017**, *55*, 70–78. [CrossRef]
22. Wu, J.; Feng, Y.; Sun, P. Sensor fusion for recognition of activities of daily living. *Sensors* **2018**, *18*, 4029. [CrossRef]
23. Roman, R.; Zhou, J.; Lopez, J. On the features and challenges of security and privacy in distributed internet of things. *Comput. Netw.* **2013**, *57*, 2266–2279. [CrossRef]
24. Weber, R.H. Internet of Things–New security and privacy challenges. *Comput. Law Secur. Rev.* **2010**, *26*, 23–30. [CrossRef]
25. Bai, G.; Yan, L.; Gu, L.; Guo, Y.; Chen, X. Context-aware usage control for web of things. *Secur. Commun. Netw.* **2014**, *7*, 2696–2712. [CrossRef]
26. Haller, S.; Karnouskos, S.; Schroth, C. The internet of things in an enterprise context. In *Future Internet Symposium*; Springer: Berlin/Heidelberg, Germany, 2008; pp. 14–28.
27. Whitmore, A.; Agarwal, A.; Da Xu, L. The Internet of Things—A survey of topics and trends. *Inf. Syst. Front.* **2015**, *17*, 261–274. [CrossRef]
28. Lu, R.; Li, X.; Liang, X.; Shen, X.; Lin, X. GRS: The green, reliability, and security of emerging machine to machine communications. *IEEE Commun. Mag.* **2011**, *49*, 28–35.
29. Kothmayr, T.; Schmitt, C.; Hu, W.; Brünig, M.; Carle, G. DTLS based security and two-way authentication for the Internet of Things. *Ad Hoc Netw.* **2013**, *11*, 2710–2723. [CrossRef]
30. Kotzanikolaou, P.; Magkos, E. Hybrid key establishment for multiphase self-organized sensor networks. In Proceedings of the Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, Taormina, Italy, 16 June 2005; pp. 581–587.
31. Moghaddam, F.F.; Moghaddam, S.G.; Rouzbeh, S.; Araghi, S.K.; Alibeigi, N.M.; Varnosfaderani, S.D. A scalable and efficient user authentication scheme for cloud computing environments. In Proceedings of the 2014 IEEE Region 10 Symposium, Kuala Lumpur, Malaysiam, 14–16 April 2014; pp. 508–513.
32. Ferrag, M.A.; Maglaras, L.A.; Janicke, H.; Jiang, J.; Shu, L. Authentication protocols for Internet of Things: A comprehensive survey. *Secur. Commun. Netw.* **2017**, *2017*. [CrossRef]
33. Saadeh, M.; Sleit, A.; Qatawneh, M.; Almobaideen, W. Authentication techniques for the internet of things: A survey. In Proceedings of the Cybersecurity and Cyberforensics Conference (CCC), Amman, Jordan, 2–4 August 2016; pp. 28–34.
34. Yue, X.; Wang, H.; Jin, D.; Li, M.; Jiang, W. Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. *J. Med. Syst.* **2016**, *40*, 218. [CrossRef]
35. Dai, H.-N.; Zheng, Z.; Zhang, Y. Blockchain for Internet of Things: A survey. *IEEE Internet Things J.* **2019**, *6*, 8076–8094. [CrossRef]

36. Trnka, M.; Cerny, T.; Stickney, N. Survey of Authentication and Authorization for the Internet of Things. *Secur. Commun. Netw.* **2018**, *2018*. [CrossRef]
37. Mukherjee, A.; Ghosh, S.; Behere, A.; Ghosh, S.K.; Buyya, R. Internet of Health Things (IoHT) for Personalized Health Care using Integrated Edge-Fog-Cloud Network. *J. Ambient Intell. Humaniz. Comput.* **2020**. [CrossRef]
38. Alam, T. mHealth Communication Framework using blockchain and IoT Technologies. *Int. J. Sci. Technol. Res.* **2020**. [CrossRef]
39. Rathee, G.; Sharma, A.; Saini, H.; Kumar, R.; Iqbal, R. A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. *Multimed. Tools Appl.* **2020**, *79*, 9711–9733. [CrossRef]
40. Patel, V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Inform. J.* **2019**, *25*, 1398–1411. [CrossRef] [PubMed]
41. Chen, Y.; Ding, S.; Xu, Z.; Zheng, H.; Yang, S. Blockchain-based medical records secure storage and medical service framework. *J. Med. Syst.* **2019**, *43*, 5. [CrossRef] [PubMed]
42. Chakraborty, S.; Aich, S.; Kim, H.-C. A secure healthcare system design framework using blockchain technology. In Proceedings of the 2019 21st International Conference on Advanced Communication Technology (ICACT), PyeongChang, Korea, 17–20 February 2019; pp. 260–264.
43. Zhang, A.; Lin, X. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. *J. Med. Syst.* **2018**, *42*, 140. [CrossRef]
44. Rahmadika, S.; Rhee, K.-H. Blockchain technology for providing an architecture model of decentralized personal health information. *Int. J. Eng. Bus. Manag.* **2018**. [CrossRef]
45. Zhang, J.; Xue, N.; Huang, X. A secure system for pervasive social network-based healthcare. *IEEE Access* **2016**, *4*, 9239–9250. [CrossRef]
46. Hasselgren, A.; Kralevska, K.; Gligoroski, D.; Pedersen, S.A.; Faxvaag, A. Blockchain in healthcare and health sciences—A scoping review. *Int. J. Med. Inform.* **2020**, *134*, 104040. [CrossRef]
47. Agbo, C.C.; Mahmoud, Q.H.; Eklund, J.M. Blockchain technology in healthcare: A systematic review. In *Healthcare*; Multidisciplinary Digital Publishing Institute: Basel, Switzerland, 2019; p. 56.
48. Ferrag, M.A.; Maglaras, L.; Derhab, A. Authentication and authorization for mobile IoT devices using biofeatures: Recent advances and future trends. *Secur. Commun. Netw.* **2019**. [CrossRef]
49. Granjal, J.; Monteiro, E.; Silva, J.S. Security for the internet of things: A survey of existing protocols and open research issues. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 1294–1312. [CrossRef]
50. Meddeb, A. Internet of things standards: Who stands out from the crowd? *IEEE Commun. Mag.* **2016**, *54*, 40–47. [CrossRef]
51. Weyrich, M.; Ebert, C. Reference architectures for the internet of things. *IEEE Softw.* **2016**, *33*, 112–116. [CrossRef]
52. Zhang, M.; Sun, F.; Cheng, X. Architecture of internet of things and its key technology integration based-on RFID. In Proceedings of the 2012 Fifth International Symposium on Computational Intelligence and Design, Nanjing, China, 18–20 October 2012; pp. 294–297.
53. Gou, Q.; Yan, L.; Liu, Y.; Li, Y. Construction and strategies in IoT security system. In Proceedings of the 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, Beijing, China, 20–23 August 2013; pp. 1129–1132.
54. Zhao, K.; Ge, L. A survey on the internet of things security. In Proceedings of the 2013 Ninth International Conference on Computational Intelligence and Security, Emeishan, China, 14–15 December 2013; pp. 663–667.
55. Castellani, A.P.; Bui, N.; Casari, P.; Rossi, M.; Shelby, Z.; Zorzi, M. Architecture and protocols for the internet of things: A case study. In Proceedings of the 2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), Mannheim, Germany, 29 March–2 April 2010; pp. 678–683.
56. Anshel, I.; Anshel, M.; Goldfeld, D.; Lemieux, S. Key agreement, the Algebraic EraserTM, and lightweight cryptography. *Contemp. Math.* **2007**, *418*, 1–34.
57. Artin, E. Theory of braids. *Ann. Math.* **1947**, *48*, 101–126. [CrossRef]
58. Hong, D.; Sung, J.; Hong, S.; Lim, J.; Lee, S.; Koo, B.; Lee, C.; Chang, D.; Lee, J.; Jeong, K. HIGHT: A new block cipher suitable for low-resource device. In Proceedings of the CHES 2016, Barbara, CA, USA, 17–19 August 2016; pp. 46–59.
59. Li, N.; Liu, D.; Nepal, S. Lightweight Mutual Authentication for IoT and Its Applications. *IEEE Trans. Sustain. Comput.* **2017**, *2*, 359–370. [CrossRef]

60. Hoffstein, J.; Pipher, J.; Silverman, J.H. *International Algorithmic Number Theory Symposium*; Springer: Berlin, Germany, 1998; pp. 267–288.
61. Perlner, R.A.; Cooper, D.A. Quantum resistant public key cryptography: A survey. In Proceedings of the 8th Symposium on Identity and Trust on the Internet, Gaithersburg, MD, USA, 14–16 April 2009; pp. 85–93.
62. Gura, N.; Patel, A.; Wander, A.; Eberle, H.; Shantz, S.C. Comparing elliptic curve cryptography and RSA on 8-bit CPUs. In Proceedings of the CHES 2004, Cambridge, MA, USA, 11–13 August 2004; pp. 119–132.
63. Hankerson, D.; Menezes, A.J.; Vanstone, S. *Guide to Elliptic Curve Cryptography*; Springer Science & Business Media: New York, NY, USA, 2006.
64. Liu, A.; Ning, P. TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks. In Proceedings of the 7th International Conference on Information Processing in Sensor Networks, St. Louis, MO, USA, 10–13 August 2008; pp. 245–256.
65. Hermans, J.; Peeters, R.; Preneel, B. Proper RFID privacy: Model and protocols. *IEEE Trans. Mob. Comput.* **2014**, *13*, 2888–2902. [CrossRef]
66. Lee, Y.K.; Batina, L.; Singelée, D.; Verbauwhede, I. Low-cost untraceable authentication protocols for RFID. In Proceedings of the Third ACM Conference on Wireless Network Security, Hoboken, NJ, USA, 22–24 March 2010; pp. 55–64.
67. Lee, Y.K.; Batina, L.; Verbauwhede, I. EC-RAC (ECDLP based randomized access control): Provably secure RFID authentication protocol. In Proceedings of the 2008 IEEE International Conference on RFID, Las Vegas, NV, USA, 3–10 March 2008; pp. 97–104.
68. Lee, Y.K.; Batina, L.; Verbauwhede, I. Untraceable RFID authentication protocols: Revision of EC-RAC. In Proceedings of the 2009 IEEE International Conference on RFID, Orlando, FL, USA, 27–28 April 2009; pp. 178–185.
69. Ko, K.; Lee, S.; Cheon, J.; Han, J.; Kang, J.-S.; Park, C. New public-key cryptosystem using braid groups. In Proceedings of the Advances in Cryptology—CRYPTO 2000, Santa Barbara, CA, USA, 20–24 August 2000; pp. 166–183.
70. Anshel, I.; Anshel, M.; Fisher, B.; Goldfeld, D. New key agreement protocols in braid group cryptography. In *Cryptographers' Track at the RSA Conference*; Springer: Berlin/Heidelberg, Germany, 2001; pp. 13–27.
71. Ko, K.H.; Choi, D.-H.; Cho, M.S.; Lee, J.-W. New Signature Scheme Using Conjugacy Problem. *IACR Cryptol. ePrint Arch.* **2002**, *2002*, 168.
72. Lee, E.; Lee, S.; Hahn, S. Pseudorandomness from braid groups. In Proceedings of the Advances in Cryptology—CRYPTO 2001, Santa Barbara, CA, USA, 19–23 August 2001; pp. 486–502.
73. Hofheinz, D.; Steinwandt, R. A practical attack on some braid group based cryptographic primitives. In Proceedings of the Public Key Cryptography 2003, Miami, FL, USA, 6–8 January 2003; pp. 187–198.
74. Lee, S.; Lee, E. Potential weaknesses of the commutator key agreement protocol based on braid groups. In Proceedings of the Advances in Cryptology—EUROCRYPT 2002, Amsterdam, The Netherlands, 28 April–2 May 2002; pp. 14–28.
75. Ben-Zvi, A.; Blackburn, S.R.; Tsaban, B. A practical cryptanalysis of the Algebraic Eraser. In Proceedings of the Annual Cryptology Conference, 2016, Santa Barbara, CA, USA, 14–18 August 2016; pp. 179–189.
76. Blackburn, S.R.; Robshaw, M.J. On the security of the Algebraic Eraser tag authentication protocol. In Proceedings of the International Conference on Applied Cryptography and Network Security 2016, London, UK, 19–22 June 2016; pp. 3–17.
77. Kalka, A.; Teicher, M.; Tsaban, B. Short expressions of permutations as products and cryptanalysis of the Algebraic Eraser. *Adv. Appl. Math.* **2012**, *49*, 57–76. [CrossRef]
78. Peeters, R.; Hermans, J.; Fan, J. IBIHOP: Proper Privacy Preserving Mutual RFID Authentication. *RFIDSec Asia* **2013**, *11*, 45–56.
79. Vaudenay, S. On privacy models for RFID. In Proceedings of the Advances in Cryptology–ASIACRYPT 2007, Kuching, Malaysia, 2–6 December 2007; pp. 68–87.
80. Zhu, H.; Lin, X.; Zhang, Y.; Lu, R. Duth: A user-friendly dual-factor authentication for Android smartphone devices. *Secur. Commun. Netw.* **2015**, *8*, 1213–1222. [CrossRef]
81. Chen, D.; Zhang, N.; Qin, Z.; Mao, X.; Qin, Z.; Shen, X.; Li, X.-Y. S2M: A lightweight acoustic fingerprints-based wireless device authentication protocol. *IEEE Internet Things J.* **2017**, *4*, 88–100. [CrossRef]
82. Katz, J.; Lindell, A.Y. Aggregate message authentication codes. In *Topics in Cryptology–CT-RSA 2008*; Springer: Berlin, Germany, 2008; pp. 155–169.

83. Lai, C.; Li, H.; Lu, R.; Jiang, R.; Shen, X. LGTH: A lightweight group authentication protocol for machine-type communication in LTE networks. In Proceedings of the Global Communications Conference (GLOBECOM) 2013, Atlanta, GA, USA, 9–13 December 2013; pp. 832–837.
84. Lai, C.; Lu, R.; Zheng, D.; Li, H.; Shen, X.S. GLARM: Group-based lightweight authentication scheme for resource-constrained machine to machine communications. *Comput. Netw.* **2016**, *99*, 66–81. [CrossRef]
85. Lee, S.-H.; Jeong, Y.-S. Information authentication selection scheme of IoT devices using conditional probability. *Indian J. Sci. Technol.* **2016**. [CrossRef]
86. Endler, M.; Briot, J.-P.; De Almeida, V.; Dos Reis, R.; Silva, F.S.E. Stream-based Reasoning for IoT Applications–Proposal of Architecture and Analysis of Challenges. *Int. J. Semant. Comput.* **2017**, *11*, 325–344. [CrossRef]
87. Borgohain, T.; Borgohain, A.; Kumar, U.; Sanyal, S. Authentication systems in internet of things. *arXiv* **2015**, arXiv:1502.00870.
88. Alonso, Á.; Fernández, F.; Marco, L.; Salvachúa, J. Iaacaas: Iot application-scoped access control as a service. *Future Internet* **2017**, *9*, 64. [CrossRef]
89. Cirani, S.; Picone, M.; Gonizzi, P.; Veltri, L.; Ferrari, G. Iot-oas: An oauth-based authorization service architecture for secure services in iot scenarios. *IEEE Sens. J.* **2014**, *15*, 1224–1234. [CrossRef]
90. Kumari, A.; Gupta, R.; Tanwar, S.; Kumar, N. Blockchain and AI amalgamation for energy cloud management: Challenges, solutions, and future directions. *J. Parallel Distrib. Comput.* **2020**, *143*, 148–166. [CrossRef]
91. Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M. On blockchain and its integration with IoT. Challenges and opportunities. *Future Gener. Comput. Syst.* **2018**, *88*, 173–190. [CrossRef]
92. Zheng, Z.; Xie, S.; Dai, H.-N.; Chen, W.; Chen, X.; Weng, J.; Imran, M. An overview on smart contracts: Challenges, advances and platforms. *Future Gener. Comput. Syst.* **2020**, *105*, 475–491. [CrossRef]
93. Fan, K.; Wang, S.; Ren, Y.; Li, H.; Yang, Y. Medblock: Efficient and secure medical data sharing via blockchain. *J. Med. Syst.* **2018**, *42*, 136. [CrossRef]
94. Li, H.; Zhu, L.; Shen, M.; Gao, F.; Tao, X.; Liu, S. Blockchain-based data preservation system for medical data. *J. Med. Syst.* **2018**, *42*, 141. [CrossRef]
95. Zubaydi, H.D.; Chong, Y.-W.; Ko, K.; Hanshi, S.M.; Karuppayah, S. A review on the role of blockchain technology in the healthcare domain. *Electronics* **2019**, *8*, 679. [CrossRef]
96. Automated Validation of Internet Security Protocols and Applications (AVISPA) Tool. Available online: http://www.avispa-project.org/ (accessed on 15 March 2020).
97. Chicxurug. SolMet-Solidity-Parser. Available online: https://github.com/chicxurug/SolMet-Solidity-parser (accessed on 20 February 2020).
98. Singh, A.; Chatterjee, K. A secure multi-tier authentication scheme in cloud computing environment. In Proceedings of the 2015 International Conference on Circuit, Power and Computing Technologies (ICCPCT), Nagercoil, India, 19–20 March 2015; pp. 1–7.
99. Yang, J.H.; Lin, P.Y. An ID-based user authentication scheme for cloud computing. In Proceedings of the 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), Kitakyushu, Japan, 27–29 August 2014; pp. 98–101.
100. Raza, S. *Lightweight Security Solutions for the Internet of Things*; Mälardalen University: Västerås, Sweden, 2013.