INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

A BlockChain-Based IoT Data Securing and Sharing System for Attendance Management

Atowar Ul Islam[1]*, **Samarjit Das**[2], **Aniruddha Deka**[3], **Chinmoy Bharadwaj**[1], **Priyanka Sarma**[1]

1 Department of Computer Science, University of Science & Technology, Ri-Bhoi, 793101, Meghalaya, India
2 Department of CSE, The Assam Royal Global University, Guwahati, 781035, Assam, India
3 Department of Computer Science and Engineering, Assam Down Town University, Panikhaiti, Guwahati, 781026, Assam, India

OPEN ACCESS

Received: 05-08-2023

Accepted: 20-05-2024

Published: 08-06-2024

Citation: Islam AU, Das S, Deka A, Bharadwaj C, Sarma P (2024) A BlockChain-Based IoT Data Securing and Sharing System for Attendance Management. Indian Journal of Science and Technology 17(23): 2430-2443. https://doi.org/10.17485/IJST/v17i23.1981

* **Corresponding author**.

atowar91626@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objective: An Internet of Things (IoT) network has constraints on power consumption, processing power and security of end devices in the network. On the other hand, blockchain technology has some difficulties in storage capacity, data privacy, the ability to revoke consent, energy usage, scalability, and speed. To overcome the individual limitations of these two technologies, we integrate these two to propose a new design with an intention to authenticate, secure and share data pertaining to attendance system. In this present work the primary implementation details of our proposed work regarding coding are analyzed and a straightforward solution is offered by using indexing. **Methods**: Through our proposed work we introduce a multifaceted authentication system for user device substantiation, a Public Key Infrastructure (PKI) and RSA (Rivest-Shamir-Adleman) based blockchain implementation for data sharing and a rule-based access control scheme used for accessing data. **Findings**: The system can work with unidirectional and bidirectional IoT networks, and the data is stored on blockchain, providing more security to the data generated on the IoT network. Blockchain technology is utilized to offer a solution for certain problems encountered within a widespread network. Furthermore, a multi-factor authentication scheme is introduced and a rule-based access control scheme to access the data. **Novelty:** The blockchain is emerging which can be used to decentralize management and protect sensitive data. In a blockchain based attendance system, no administrative authority is permitted to modify or erase data. The individual who adds a data entry to the blockchain cannot later deny their involvement in the action. On the blockchain, all of the data and history are accessible to every participant. The blockchain based attendance system needs to offer a database that can be trusted, secure, and impossible to manipulate.

Keywords: Blockchain (BC); Internet of Things (IoT); Student Attendance Management (SAM); User Authentication Key (UAK); Data Sharing

1 Introduction

Information technology has altered many aspects of the way educational systems operate over the years and made life easier for students, parents, academic and non-academic staffs and management in certain areas like examinations, fee processing etc. Manual methods have many shortcomings in marking in registers which may cause error in certain situations specially in monitoring students' attendance both in the classroom and in the lab. Radio Frequency Identification (RFID) based smart cards and biometric technologies, including fingerprint, iris, barcode, and facial recognition, have been used in Securing IoT with Block chain-Based System (SIBS) systems. An IoT network consists of a variety of related items or intelligent things that are typically linked by the Information superhighway. IoT devices frequently receive distinctive IP numbers to aid in network device identification. These gadgets can frequently be controlled virtually and have the potential to communicate with one another. They can also collect or detect information from their immediate surroundings, which they can then transform into useful data that the system or its users can use for communication, data integrity, authentication, and data protection. Healthcare, industrial automation and manufacturing are just a few of the areas and industries where the IoT is becoming increasingly integrated into daily activities. Smart IoT devices can seamlessly integrate with their surroundings to offer timely access to various types of information and services. Block chains have undergone extensive development for the administration of digital crypto currencies like Bit-coin. The use of blockchain networks technology is a key component of these currencies. The integrity and security of financial transfers are enhanced by the distributed and decentralized character of block chains. Blockchain networks' fundamental ideas are the same regardless of whether they are permission-based or permission-less. Contrary to a permission-less blockchain, the former needs authentication, network device identification, and enrollment by the central authority, preventing users from connecting to the blockchain network directly. Blockchains operate by storing each event that takes place on a network in a block, which is a hash-based structure. A financial transfer, a change in ownership of an object like a vehicle or a bond, or an information exchange between two different participants over a network are all examples of transactions. The hash value of the previous block is contained in each block of the block chain events. The resulting ledger can then be appropriately saved in a database or flat-file.

The attendance system is made to record of attendance transaction automatically. In the current attendance system, the attendance transaction from the attendance machine vendor application will be stored on the local SQL server database in each representative office, then by using the SQL Server Integration Service (SSIS) the database is collected in a centralized database for consumption. Thus, it can be said that the attendance system can be categorized as a centralized system/database that requires a central authority.

A conventional databases do not have special features in checking whether a piece of information has experienced unauthorized changes. In a relational database, data can be modified or deleted. A database administrator can make changes to any part of the data or structure. Blockchain-based attendance systems can be alternative solutions because of its capability to secure data. Apart from the many limitations of the blockchain, but to get a system with high immutability blockchain \based systems will be more profitable than if you have to improve the verification technology and data storage on centralized systems[1]. On a blockchain based system, there is no administrator permission that allows editing or deleting data. Someone who enters an information entry on the blockchain will not be able to deny that he is doing the activity. Each party on the blockchain has access to the entire database and history.

The IoT is a relatively new prototype that has changed traditional ways of life and given individuals access to high-tech lifestyles. Smart cities, smart homes, energy conservation, pollution reduction smart industries, smart transportation etc. are just few examples of the different transmission system of IoT.[2]

Year after year, IoT is growing, with its primary aim being the advancement of 5G technologies. However, conversely as a result of the growing accessibility of the internet, IoT becomes susceptible to potential attacks from various angles, making security and privacy a difficult task[3].

Blockchain Technology is an emerging technology to infuse trust among the participating agents in a business transaction. It does so through its peculiar architectural elements. The key characteristics of the blockchain are decentralization, immutability, anonymity, and transparency. Each participant in the blockchain network stores blocks of data, thus ensuring data integrity and consistency using the various consensus algorithms. Cryptographic hash functions help in keeping the data immutable. The immutable property allows no one to alter or delete the data from a shared database.

In 2019 two significant technologies were proposed for an information system namely bitcoin and blockchain[4]. Blockchain is an openly accessible digital record-keeping system and a decentralized method of conducting transactions between individuals. They described the operational principle and structure of the blockchain in their research. Decentralizing the current centralized system and addressing numerous security concerns are effectively resolved through the implementation of blockchain technology. The blockchain is expanding in size. As a result, there exists a difficulty in efficiently storing and validating. Task scheduling is a difficult task in the distribution of the blockchain network. They proposed a future assignment that involves merging IoT applications with blockchain technology.

In 2019, Alamri et al.[5] discussed the challenges faced by blockchain and the IoT in the blockcahin IoT environment, specifically in Cyber-Physical Systems and telemetry systems. They highlighted the difficulties in integrating blockchain with 4G/5G broadband communications. The researchers suggested that blockchain currently has limited applications and is primarily used in the field of encrypted currencies. However, they believe that utilizing blockchain can enhance the compatibility between the IoT and blockchain technology.

Integration of blockchain with data analytics techniques is often recommended to build next-generation data-driven networks[6]. The evolution in data communication, mobile technology, and wireless sensor technologies has opened up new avenues to build data-driven applications. But maintaining security and privacy and building trustworthy applications on top of such networks is one of the biggest challenges. Blockchain technologies provide a trust layer that can leverage to build dependable applications. Such an integrative approach of data-driven blockchain has been used to build applications for smart grid system[7] and in water consumption management and supply-chain management also used blockachain technology[8].

The field of tracking and tracing is concerned with determining the location of a unit, such as a product or gadget, both at present and at past locations at various times. For upcoming analysis, information about the unit's placements will be kept in a dynamic database. These systems occasionally have the capacity to save data and detailed information on the product's departure or arrival at a specified location. The position of an object, its identity, and the moment of a transition may all be included in the saved data.

Tracking systems are one of the best examples of services and apps that use blockchain technology in conjunction that have surfaced recently. Several studies have recommended using blockchain technology. A blockchain has been used to create a framework that can perform tracking operations. A number of ideas have been proposed to enhance unit traceability. Even though some of the recommended systems have achieved high levels of traceability, they still have issues with usability, security, and implementation ease. Some other systems have made use of other technologies and/or methods to achieve similar aims.

Here in the proposed system uses role-based data access control integrated with IoT. The main goal is to always be able to connect to the web server and send or receive data transactions to the blockchain, which improves web server performance and adds security to the system. Additionally, develop a blockchain architecture that offers user-friendly functionality. The remainder of the essay is structured as follows. The relevant work with a research gap is included in section-2. Definition and different issues are described in section -3. Methodologies are presented in Section-4. The results of the studies are presented in Section-5. Comparative analysis of the paper is depicted in Section-6. Conclusion and future prospects are discussed in section 7.

2 Literature Survey

Attendance monitoring system like Biometric-based face recognition, fingerprint, and even iris-based attendance systems are available in the market. Similarly, device-based attendance systems like Smart Cards and RFID-based attendance systems are available in the market as products. These various attendance recording techniques are acceptable in various different scenarios and are practically deployed in offices, institutions, laboratories, factories, etc. Ardina, H., & Nugraha, I. G. B. B. (2019) developed a blockchain-based employee attendance system to manage attendance transactions so that the stored data can be maintained for its integrity and reliability[9]. Yang Wenly et. al[10] explores a blockchain-based mechanism to improve traditional Internet services, focusing on features like autonomous processing, smart contractual enforcement, and traceable transactions. The researchers provide a comprehensive review of the blockchain-based framework for developing decentralized protocols for various Internet services. The survey aims to address the integration of blockchain technology to enhance the security of Internet services and identify the critical requirements for creating a decentralized and trustworthy Internet service. The proposed[11] tracking system aims to address the limitations of current systems by utilizing blockchain technology. The system incorporates important characteristics such as accountability, authorization, audit-ability, integrity, punctuality, and honesty to ensure its effectiveness. The design of the system is based on QuarkChain, a flexible and scalable blockchain infrastructure that uses a sharded blockchain protocol and a two-layer architecture. The authors also discussed the complete architecture, implementation methodology, and system design of the proposed tracking system. Overall, the proposed system offers a solution to the challenges of real-time traceability, inefficiency, and manual errors faced by existing systems, by leveraging blockchain technology and incorporating key features for a robust tracking system.

Stochastic simulation has been proposed by Xie Wei et al.[12] to influence the architecture of the blockchain, protecting pharmaceutical supplies against theft, temperature diversion, and counterfeiting while enhancing the responsiveness, efficiency, and dependability of the supply chain. Their method performs promisingly, as the early empirical study shows.

A private blockchain designed by Priyanka B. Dongre et al.[13] which enables different system users to carry out their operations in accordance with the guidelines or smart contracts specified while they are a part of the blockchain. They have created a private blockchain architecture that employs QR Codes, SHA-256 algorithm, and a unique technique to build blocks and store data in the blockchain for a specific amount of time. The use case used to illustrate the proposed private blockchain framework is the marking of student attendance with mobile phones and instructor laptops that contribute to the blockchain's construction. This innovation in blockchain technology has the potential to revolutionize various industries by providing a secure and efficient system for decentralized activities.

Van Dung Nguyen et al.[14] have been compared the advantages/disadvantages of existing smart attendance management systems. They designed an IoT-based intelligent attendance management system based on the cloud, a web server, Google API, a non-contact body temperature sensor, and the Raspberry Pi 4 module (4G). They also done a survey at a university and summarized the satisfaction levels of using their system.

Ahmed Ali Talib et al.[15] carried out the study of integration of IoT and block-chain in relation with different issues, opportunities, and application area.

Islam A. et al.[16] proposed a IoT based device which main objective is to develop an intelligent monitoring and automated irrigation system that minimizes water use based on individual conditions and enables real-time environmental.

Singh A. et al.[17] have been proposed a protocol called ES-CLAKA has been developed for WBANs (Wireless Body Area Networks) using blockchain technology. This protocol ensures both efficiency and security, meeting various security requirements. The ES-CLAKA protocol has undergone a formal analysis using the BAN logic and the ROR model, which has confirmed the security of the authenticated key-establishment phase and the confidentiality of the established key. The findings indicate that ES-CLAKA, when compared to other highly effective CLAKA protocols, requires 47.4% less computational time, 20% less communication bandwidth, and 16.67% less storage overhead, all while assuming reasonable conditions.

For the purpose of detecting faults in IoT, a novel technique called Blockchain Assisted Data Edge Verification with Consensus Algorithm for Machine Learning (BDEV-CAML) is created and proposed by Vaiyapuri T. et al.[18]. The BDEV-CAML technique proposed combines the advantages of blockchain, the IoT, and machine learning (ML) models in order to improve the trustworthiness, effectiveness, and security of the IoT network. The deep directional gated recurrent unit (DBiGRU) model is employed for the purpose of identifying faults in the IoT network. To enhance the fault detection rate, the African vulture optimization algorithm (AVOA) technique is employed in tuning the DBiGRU model's hyperparameters.

A unique Blockchain-based Approval Process System (BAPS) has been proposed by Gandhi Sanil et al.[19] in an effort to build mutual trust between the approving authorities and the submitter. It securely stores the information on a platform that cannot be altered, addressing one of the main drawbacks of traditional paper-based systems.

Blockchain technology has been used by Hanggoro Delphi et al.[20] to store HR department employee attendance data. They selected Hyperledger Composer due to the quick validation time of blockchain technology. In the result part Hyperledger Composer performance is measured by evaluating block transaction times.

An algorithm to generate a hash based on chaos theory (1D and 2D) logistic maps and the new Merkle-Damgård construction has been proposed by Kamal Ali Zainab et al.[21].The hash outputs undergo testing concerning collision, complexity, and time. The Jaccard similarity and other coefficient measurements are used to evaluate the proposed algorithm, and the results show that the similarity between the inputs and outputs is not greater than 0.1932 percent.

Based on the research mentioned above, it has been observed that various techniques are employed by researchers to implement attendance systems utilizing blockchain technology. They also engaged in a discussion about clouds and their utilization as servers for storing records through the IoT. However, we have discovered that authors did not utilize IoT, blockchain, and cloud servers simultaneously. The proposed system integrates role-based data access control with IoT. The primary objective is to consistently establish a connection with the web server and facilitate the exchange of data transactions on the blockchain. This enhances the performance of the web server while enhancing the security of the system. Furthermore, create a user-friendly blockchain framework that provides functional features.

3 Definition and Issues

3.1 Blockchain:

A crucial component of the system is that blockchain is an immutable database that organizes all activities into blocks. All data transfers made by regular nodes for each session started by the supervisory nodes are recorded on the blockchain. The timestamp, mac_id, user information, prior block hash code, and next block hash code are all included in each transaction in the block. The previous hash and next hash codes make it simple to distinguish between the previous and subsequent blocks in a linked list of all the data recorded in the blockchain. The HTTP protocol is used by the Web server to interact with the blockchain. The blockchain is accessible to the master node, the supervising nodes, and other nodes via a web server. The web server on a bidirectional IoT network can provide access to the blockchain for the regular nodes. The blockchain cannot be accessed by regular peers in a unidirectional network.

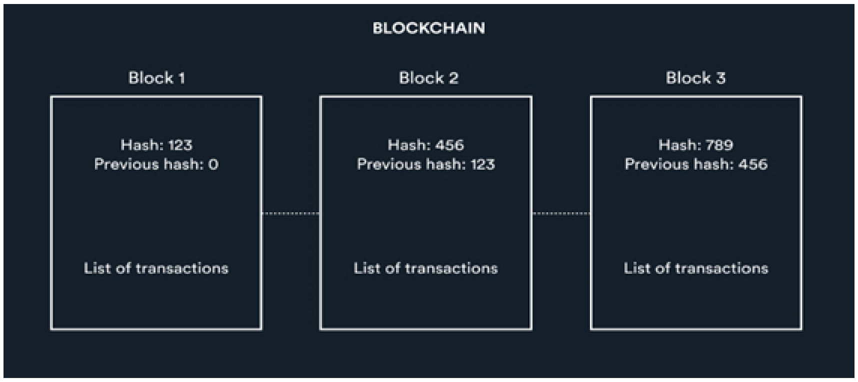


Fig 1. Structure of blockchain

3.2 Blockchain technology in larger network issues:

Blockchain has some difficulties in a small setup, despite the fact that it is receiving more focus and being used to increase data security in several attacks. The blockchain handles a variety of tasks, including redundancy checking, conventional database processing, and consensus mechanisms, which can cause slow performance. Large storage space, computational power, and bandwidth needs increase with the size of the blockchain network. For each public key, every activity on the blockchain is transparent. The public key, however, can help it maintain some level of anonymity. The publicly accessible nature of blockchain makes that data accessible to every node on the network. Every node on the network can obtain that data due to block chain's open accessibility. Large amounts of energy and computing power are used during the creation of a public blockchain's blocks.

Numerous end products, such as smartphones, laptops, RFI cards, fingerprint scanners, computers, etc., are included in the system. These gadgets are all a component of an IoT network that is both unidirectional and bidirectional.

Ordinary Node, Supervisory Node, and Master Node are the three categories assigned to the system's users. Each of these users has particular access privileges that have been defined by policy.

4 Methodology

The suggested method Utilizing IoT and the blockchain idea, SIBS, is a powerful system for secure and authenticated data sharing. The suggested system architecture is depicted in Figure 2. Block chain, the IoT network, web servers, and end consumers are the main system's building blocks.

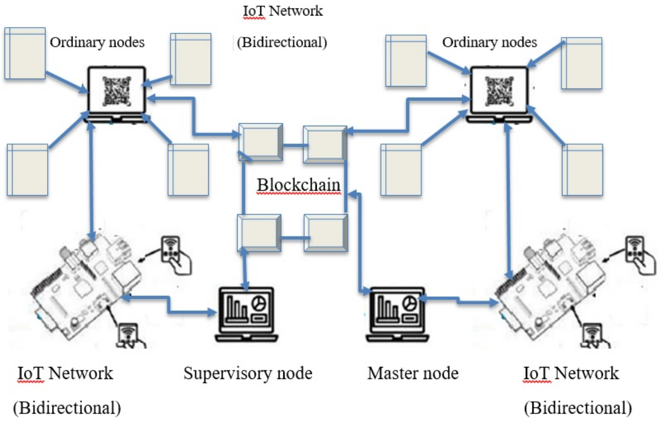


Fig 2. System Architecture

Numerous gadgets, including mobile phones, RFID card readers, RFID tags, etc., are part of IoT networks. Through a web server, a block chain records all data transactions. The people who share data and communicate via a web server using the IoT and blockchain networks are known as nodes. Ordinary, supervising, and master nodes are the different categories for the nodes. The complete block chain network is managed by the master node. The supervising nodes can be added or removed by the master node, and it also chooses how many IoT networks each supervisory node can control. The supervising nodes can also be added or removed by the master node. Additionally, an IoT network can be removed or assigned to a monitoring node by the master node. The different technique of the methods are described bellow.

4.1 Use cases:

The suggested lightweight blockchain framework for IoT networks has a defined use case. In an institution, for instance, the system is used by students, teachers, and the management. These users can be thought of as nodes that ask a web server for the necessary service using end devices in an IoT network. These nodes' functions in requesting to carry out a transaction on the blockchain network are outlined here.

4.2 IoT network:

The IoT networks come in two flavours: unidirectional and bidirectional. In contrast to the bidirectional IoT network, which creates two-way traffic, the unidirectional IoT network only produces one-way traffic. Only when the supervisory node allows the data write operation for ordinary nodes can each device connected to an IoT network start a data write operation. The data write transaction can be started by the regular node linked to a unidirectional IoT network via the supervisory node. The Raspberry Pi gathers data from the network-connected devices in a unidirectional IoT network by connecting the regular nodes to it and acting as a bridge between the private network and the monitoring node. Only authenticated ordinary nodes are permitted to link to the blockchain and start data write transactions, according to the supervisory node. Only a web server or supervisory node can start a data read operation from the blockchain on behalf of regular nodes like smartphones.

4.3 Unidirectional IoT network:

An RFID Reader, an RFID tag, a fingerprint scanner, and other devices are part of the unidirectional IoT network that is constructed around a Raspberry Pi Gateway. Due to their low computing capacity, these devices cannot immediately access the blockchain. The supervisory server and these IoT devices communicate through the Raspberry Pi Gateway. Only data transactions from devices linked to the unidirectional network are permitted when the supervisory node starts the data record session for the IoT network. Every transaction started by these devices is therefore recorded on the Raspberry Pi Gateway and added to the blockchain by the supervising node.

4.4 Bidirectional IoT network:

Smartphones, laptops, and PCs, among other data-sending and receiving hardware, are part of the bidirectional network. When the supervisory node starts the session with the ordinary nodes in this network, the ordinary nodes can start the data write operation. The ordinary node scans the QR code that the supervisory node generates and shows to start the transaction that is added to the Block chain. The regular nodes in this IoT network can access the blockchain data by sending an HTTP request to the web server.

4.5 Mathematical approach:

The assessment of the functionality and limitations of blockchain technology in IoT applications is examined by employing a mathematical framework. One way to ensure high security for IoT applications is by utilizing networks to create a series of computational tasks. Moreover, the transfer of computational tasks is accomplished by employing a transaction procedure for offloading, which involves a limited number of computational nodes[22] [23], as explained in Equation (1).

$$IB_i = \sum_{i=1}^{n} \left(D_{ij} + tr_i\right) \tag{1}$$

where,

D_{ij} indicates blockchain cluster head and tr_i represents the number of transactions.

The equation written above (Equation (1)) indicates that in order to maintain efficient computational processes at different time intervals, it is necessary to minimize the combined value of the cluster head and transactions. If the number of cluster heads is not decreased, Equation (2) demonstrates the deceleration of transaction block volume.[24]

$$p_i(i) = minm\sum_{i=1}^{n}\left(of_i * t_x(i)\right)/t_r(i) \tag{2}$$

where,

of_i denotes number of offloading tasks, t_x indicates data size of transaction blocks and t_r represents rate of transmission blocks.

Equation (2) computes the overall latency experienced in situations where Internet of Things applications are offloaded while accounting for transaction blocks with different sizes. Establishing a consistency ratio is required even in cases when the system is built using **Equation (3)** and has several data segments in its architecture[25][26].

$$CS_i(i) = minm\sum_{i=1}^{n}\left(UB_i - t_c(i)\right)/t_c(i) - 1 \tag{3}$$

where,

UB_i indicates random block transmissions and $t_c(i)$ denotes total number of operational factors in each block.

If consistency is essential in IoT applications, Equation (3) demonstrates that the established ratio should not exceed the threshold value of 0.1. Utilizing **equation (4)**, a load balancing tactic is established in the following manner. If the ratio values exceed the specified threshold values, it will not be possible to maintain consistency in the transmission of data blocks.

The above mathematical approaches are used to minimize the number of computational blocks and offloading tasks.

4.6 Algorithm:

The Algorithm-1 creates users who may be an approver or proposal

```
Algorith-1: Create User
Step-1: Start
Step-2: Input the User name as firtst_name(str), Last_name(str), role(str) and id(str).
Step-3: Create_user if (YES)
Create_user update []
Else
Return
End if
Step-4: Stop
```

We have present a simple algorithm for attendance system. If name is not registered, there will be shown the error message “name does not exist.” If the name is registered, the function will change the total current presence and increase the attendance by 1.

```
Algoritm-2: Update Attendance
Step-1: Start
Step-2: Define function as Presence (press), get (Access_attendance)
Step-3 Put attendance
Step-4: If attendance_exit then
Get_response and Register_attendance and increase by 1.
Else
Error in attendance and not register_attendance.
End If
Step-5: Stop
```

Here present an algorithm for attendance system using public key. Using Public Key Infrastructure (PKI), the user can approve or reject the procurement based on the information provided in the attendance system. The Algorithm 3 Upd_Apprv _list() is used by the approving the authority with the authority’s public key.

```
Algorithm-3: An algorithm for attendance system using public key.
Input: Approval Obj(Map) and Obj(Map) using docHah
Output: N$oti$_fication[hash].status = Approved
Step-1: Start
Step-2: Define function as Presence (press), get (Access_attendance)
Step-3: Put attendance for validation
Step-4: Check Att_Status
```

```
If Staus= pending then
    Create Noti_fication Obj and send on Noti_fication_list[].
Else
Upd_Apprv_list[]
End If
Step-5: Stop.
```

The algorithm -4 assigns a timestamp to every attendance. The approval attendance should create on time within the pre-defined time limit.

```
Algorithm 4 Algorithm to Set Time Limit.
Step-1: Fetch Att_status
Step-2: Allocate Time_stamp=T.Time_stamp
Step-3: Allocate EApproval= T. EApproval
Step-4: Allocate Curr_Appoval= T.CurrApproval
Step-5 Call Approval and Store Current_Time.
a) If on Time then
Store Status
b) Else If Not then
Not approval
c) Else
Curr_Approval= E.Approval then
Change Status and Expire.
End If
End If
Step-6: Stop
```

```
Algorithm-5: PKI-RSA Algorithm:
Step-1: Start
Step-2: Generate Key
a) Select distinct p € x, y where p is prime number.
b) A= x×y, A is used as the modules for both the public and private keys
c) Compute Euler's totient function $\partial(A)=(x-1) \times (y-1)$
d) $1<i< \partial (n)$ and e is co-prime with $\partial (n)$, e is the public exponent and i is an integer.
e) $D_n$ = inverse of e % $\partial (n)$ is a private exponent.
Step-3 Generate public and private keys
a) e, n public keys
b) $D_n$, n private keys
Step-4 Encryption –
a) Sender encrypt the message followed by step 4(b)
b) $P \equiv N^e(\%n)$ which sends to Q.
Step-5 Decryption-
a) Receiver receives the original message followed by step 5(b).
b) $N \equiv P^{Dn} \% n$
```

The foundation of a cryptosystem is the Rivest-Shamir-Adleman (RSA) algorithm. The RSA algorithm consists of encryption and decryption methods, as well as the generation of key pairs. The researchers developed a function for encrypting and decrypting messages within the system, utilizing the RSA encryption technique, which is an asymmetric-key encryption method. The researchers have also included examples of communications that should be encrypted using keys generated by RSA. Once the user has selected a message, they need to enter the specific public key in order to finish encrypting the message. The message will be encrypted and sent to the administrator, regardless of the accuracy of the public key used. The message will also include a status indicating whether the encryption was successful or unsuccessful, indicating when a user has successfully encrypted the message or attempted to do so with an incorrect public key. The encrypted message is saved with the user's account ID in the administrator's database, where the admin can decide to either decrypt the message or delete it. The administrator must enter the necessary private key in order to decrypt the message successfully.

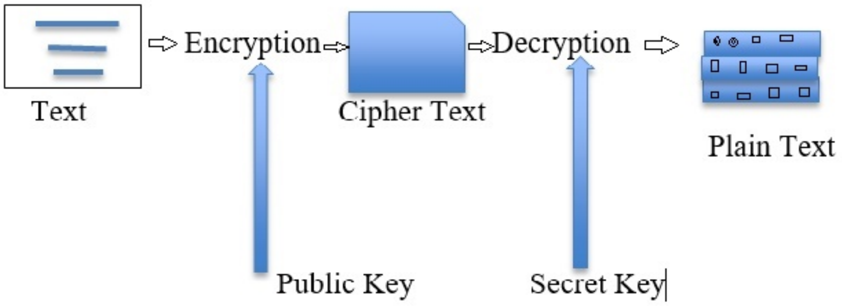


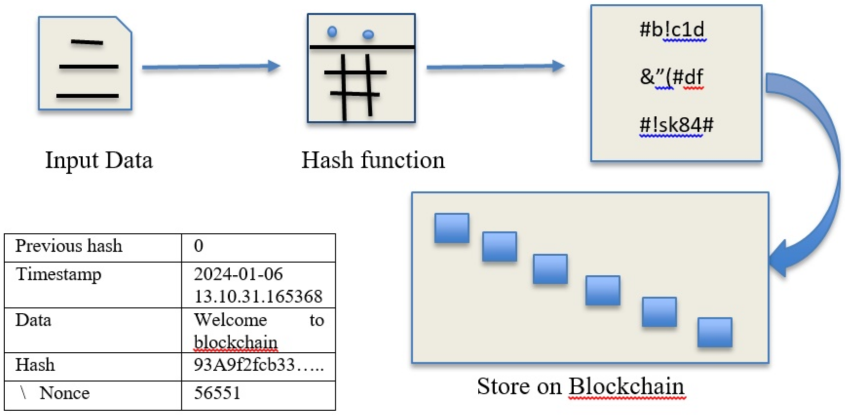
Fig 3. Encryption and Decryption process using different keys

5 Result and Discussions

Based upon user authentication, data storage, and data access schemes our system is implemented and the outputs are produced with sample input. The algorithm which are discussed in the 4.6 section, we have used in different algorithm for different purposes and here we mainly focus on algorithm-4 and algorithm-5.

5.1 User Authentication

This method uses a multi-factor authentication strategy. When a person registers on the system, the web server puts the user registration smart contract into action. When a person registers, a special private key is generated for them, and their mac address is also stored on the block chain along with their user data. The web server performs a user authentication smart contract to obtain an encrypted list of the mac IDs of approved devices when the user requests a connection to the system. In order to authenticate individuals on the network, a two-stage user authentication protocol is created. To log in using the private key, the user must first submit a request to the web server. Second, the web server performs the smart contract for user authentication to confirm the legitimacy of the user and obtain the list of approved devices. The device is authenticated and connected to the block chain once the user's private key and device mac id agree. As soon as authentication is effective, the web server adds a user session block to the block chain, allowing the user to proceed with data transactions in line with their role. Data blocks are generated first, after which they are added to the blockchain. The user data, encoded mac id, previous hash code, and distinct hash code are all contained in the data block. The preceding block's unique value in the block chain is represented by its hash code. This can be seen in the below Figure 4.



Previous hash	0
Timestamp	2024-01-06 13.10.31.165368
Data	Welcome to blockchain
Hash	93A9f2fcb33…..
\ Nonce	56551

Fig 4. Data Block added to Block chain upon Successful User Authentication

The proposed method in Figure 3 was applied to a blockchain-based transaction flow system. Each transaction is sent by more than one node. The transaction must be verified through the hash generated for it. Each time data are sent and received between the nodes, the transaction is verified through the generated hash, which must give the same hash every time. Node1 (person-1) suggests a transaction and enters it into the PKI-RSA based algorithm to give it a hash of its own (generated from the information recorded in the transaction). Node2 (person-2) checks the hash value before accepting it. If the results give the same hash value as that sent from the first node, it is accepted and sent to the other nodes. Once the transaction passes through more than one node, a decision is made after the validity of the transaction has been verified every time it is sent or received. It is then placed in the blockchain. Upon any inquiry about the transaction, it will be retrieved from the blockchain. The nodes are connected through a TCP/IP protocol in the same network, representing the number of users in a network. Nodes: - It represents the number of employees within the network.

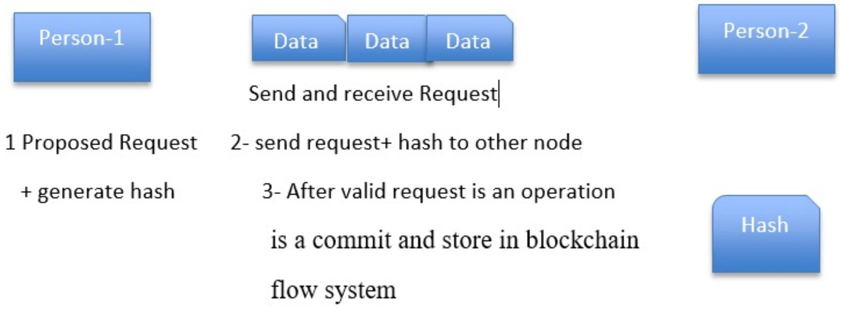
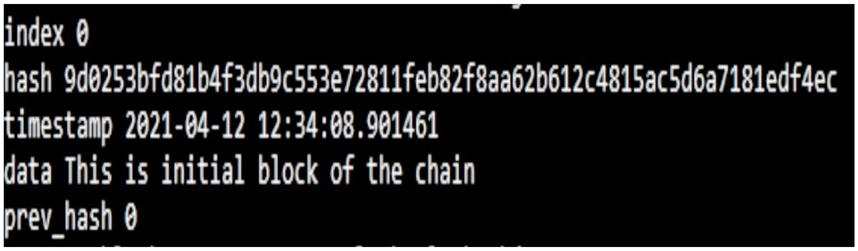

Person-1
Data
Data
Data
Person-2
Send and receive Request
1 Proposed Request
+ generate hash
2- send request+ hash to other node
3- After valid request is an operation
is a commit and store in blockchain
flow system
Hash

Fig 5. Each Node check the hash request

In terms of the significance of the suggested blockchain system, it does not permit the alteration of transactions and their corresponding hash values. If a malicious node alters a transaction, the hash values in all the stored data at that node must also be changed and modified. The change can be identified because every node operates on the same blockchain system, causing variations in hash values for a particular transaction and which provides the security in the system.

5.2 Data storage

In the blockchain, the material is stored across a number of blocks. When the web server starts the smart contract for every client in the system, a data structure is established for each transaction, and the data transaction is then recorded on the block chain. The genesis block is created by the smart contract using algoritm-1. Each data transaction produced by users after the genesis block has been created is added to the blockchain when the user completes the transaction. The Genesis block's creation is depicted in the Figure 6.



```
index 0
hash 9d0253bfd81b4f3db9c553e72811feb82f8aa62b612c4815ac5d6a7181edf4ec
timestamp 2021-04-12 12:34:08.901461
data This is initial block of the chain
prev_hash 0
```

Fig 6. Genesis's Block

Each sort of block that is created in the blockchain as a result of data exchanges takes a certain amount of time to create, as indicated in Table 1.

Table 1. Time taken for block g eneration

Block Name	Time Taken to create Block
Genesis	0.000999212
Registration	0.016958952
New Subject Creation	0.016954184
QR Code Generation	0.016955614
Mark Attendance	0.007982254

The Figure 7 shows several blocks generation time in the proposed system. It shows the graphical representation of the proposed system.

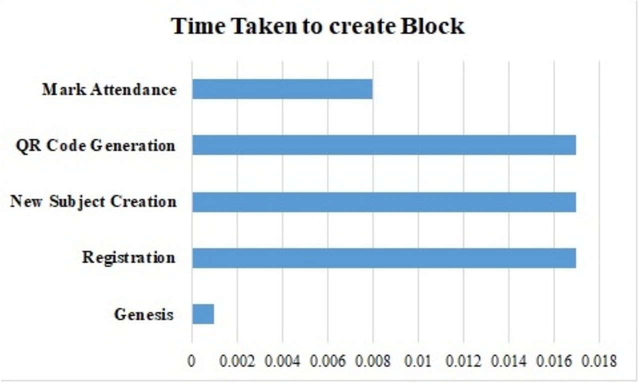


Fig 7. Time taken to generate the blocks

5.3 Data access control:

A Role-based data access control is implemented in this system. In previous sections, each system user is assigned a specific role. The system users in this work are also known as nodes. Whenever the user wants to write data or read data transactions first, the user has to connect to the web server. The web server authenticates and verifies the user's role by executing the smart contract and allows the nodes to write or read data transactions to the blockchain. As the nodes in unidirectional nodes have less computing power hence the ordinary nodes on the unidirectional networks are not directly allowed to access the blockchain, whereas the ordinary node on a bidirectional network is allowed to initiate the read operation. When the ordinary node on a bidirectional IoT network sends a request to the web server, the web server executes the smart contract to read the block chain data. Supervisory nodes can write and read the blockchain. Supervisory nodes are also responsible for writing the data on blockchain on behalf of ordinary nodes. Master nodes are allowed to read and write the data in the blockchain. For each read and write request from the supervisory node master node, the web server executes the smart contract based on the roles, and the user can perform the operations as per the policy.

In this technology, a role-based data access control is used. Each system user is given a specific function in earlier sections. In this article, the system users are also referred to as nodes. The user must establish a connection to the web server any time they want to write or receive data transactions. By executing the smart contract, the web server authenticates and validates the user's role and permits the nodes to write or receive data transactions to the blockchain. Ordinary nodes on unidirectional networks are not permitted to immediately access the blockchain because they have less computing power than ordinary nodes on bidirectional networks, which are permitted to start the read operation. The web server performs the smart contract to read the block chain data when an ordinary node on a bidirectional IoT network makes a request to it. The blockchain can be viewed and written by supervisory nodes. Additionally, supervisory nodes are in charge of recording data to the blockchain on behalf of regular nodes. The blockchain data can be viewed and written by master nodes. The web server performs the smart contract based on the roles for each read and write request from the supervisory node, master node, and the user is then free to act in accordance with the policy.

6 Comparative Analysis

A few general parameters were used to compare the proposed approach with conventional semi-automated systems, after which we compare approaches that use blockchain and IoT for attendance management. Finally, we compare the amount of time required for block chain transactions or block generation between the proposed system and systems that are solely based on block chains. It also indicates that blockchain technology is being used to provide solutions for specific issues faced in a largescale network. Table 2 demonstrates how the conventional methods are less user-friendly, have lower data accuracy, are more vulnerable, move slowly, and take more time than the suggested system[1] to[5].

Table 2. Comparison between the traditional block chain system and proposed system

Domain	Speed	System Security	Resources (Documents)	Data Acuracy	Adaptability
Traditional Blockchain System	Slow	More vulnerable	More paper work	Low	No
Proposed Blockchain system	High	Validated individuals only	Only Electronics records	High	yes

The Table 3 describes the comparison of the available systems implemented using blockchain for attendance management in terms of IoT and blockchain.

Table 3. A comparison between the existing systems and the proposed system

Author	Blockchain	IoT
J. Pereira[1]	Yes	No
Kumar S[2]	No	Yes
Sathiyanathan N[3]	No	Yes
Mohanta Bk[4]	Yes	No
Alamri M[5]	Yes	Yes
Proposed System	Yes	Yes

The above Table 3 only shows an example of comparison of proposed system how compare the work and find out the comparison chart. In the comparison chart figure we consider all the paper those are taken from the reference section.

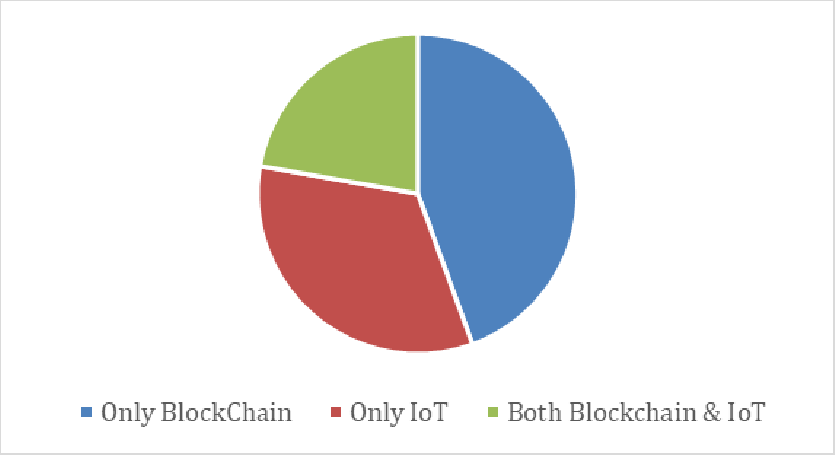


Fig 8. Comparison chart

After examining Table 3 and references, it is evident that there is a limited amount of research conducted on both blockchain technology and IoT. The majority of papers are built using only one specific technology. We have addressed both IoT and blockchain technology in our proposed system, aiming to resolve the problem of slow performance in the larger network specifically within the attendance system.

From review of literature we have find time complexity to generate the block in blockchain technology. Only few paper have mentioned time complexity to generate block in blockchain. In Table 4, it is shown that there are few popular systems build around the block chain even takes more time to generate the data block as compared to the proposed system.

After examining the data in the Table 4 mentioned, we can conclude that the generation of block time is slightly higher than our system. In comparison to other research studies, our system takes less time to generate a block in the blockchain.

Table 4. Block-Time generation comparison between existing block chain implementations and the proposed system

Blockchain Name	Block-Time
Blockchain based QR code [13]	0.217secs
Blockchain in transition system [21]	0.188 msecs
Blockchain based information sharing Security [27]	1.254 ms
Proposed	<0.210 msecs

7 Conclusions

This study have proposed a model Securing IoT with Block chain-Based System (SIBS) as user authentication, data storage, data sharing, and access control and successfully implemented an Attendance Monitoring System for Education sector by using Blockchain and IoT. The system can work with unidirectional and bidirectional IoT networks, and the data is stored on Blockchain, providing more security to the data generated on the IoT network. Furthermore, a multi-factor authentication scheme is introduced and a rule-based access control scheme to access the data. It is reflected in the results that the proposed system takes less than one (01) second time to generate the data block. Blockchain technology is utilized to offer a solution for certain problems encountered within a widespread network. Although enough work has not been performed on the use IoT and Blockchain for attendance management, we believe that this work will motivate researchers to experiment around the use case. We have also introduced some mathematical equations which minimize the offloading task of IoT device and provide high security. The detailed functions of the mathematical model is the future study of the work.

References

1) Pereira J, Tavalaei MM, Ozalp H. Blockchain-based platforms: Decentralized infrastructures and its boundary conditions. *Technological Forecasting and Social Change*. 2019;146:94–102. Available from: https://doi.org/10.1016/j.techfore.2019.04.030.
2) Kumar S, Tiwari P, Zymbler M. Internet Of Things Is A Revolutionary Approach For Future Technology Enhancement: A Review. *Journal of Big Data*. 2019;6:1–21. Available from: https://doi.org/10.1186/s40537-019-0268-2.
3) Sathiyanathan N, Selvakumar S, Selvaprasanth P. A Brief Study on IoT Applications. *International Journal of Trend in Scientific Research and Development*. 2020;4(2):23–27. Available from: https://www.ijtsrd.com/papers/ijtsrd29888.pdf.
4) Mohanta BK, Debasish J, Panda SS, Sobhanayak S. Blockchain technology: A survey on applications and security privacy Challenges. *Internet of Things*. 2019;8. Available from: https://doi.org/10.1016/j.iot.2019.100107.
5) Alamri M, Jhanjhi NZ, Humayun M. Blockchain For Internet Of Things (Iot) Research Issues Challenges And Future Directions: A Review". *International Journal of Computer Science and Network Security*. 2019;19(5):244–258. Available from: https://seap.taylors.edu.my/file/rems/publication/109566_6018_1.pdf.
6) Li H, Chen X, Guo Z, Xu J, Shen Y, Gao X. Data-driven peer-to-peer blockchain framework for water consumption management. *Peer-to-Peer Networking and Applications*. 2021;14:2887–2900. Available from: https://dx.doi.org/10.1007/s12083-021-01121-6.
7) Zeng Z, Dong M, Miao W, Zhang M, Tang H. A Data-Driven Approach for Blockchain-Based Smart Grid System. *IEEE Access*. 2021;9:70061–70070. Available from: https://dx.doi.org/10.1109/access.2021.3076746.
8) Sundarakani B, Ajaykumar A, Gunasekaran A. Big data driven supply chain design and applications for blockchain: An action research using case study approach. *Omega*. 2021;102. Available from: https://dx.doi.org/10.1016/j.omega.2021.102452.
9) Ardina H, Nugraha IGBB. Design Of A Blockchain-Based Employee Attendance System. In: and others, editor. International Conference on ICT For Smart Society (Iciss). IEEE. 2019;p. 1–4. Available from: https://doi.org/10.1109/ICISS48059.2019.8969840.
10) Yang W, Aghasian E, Garg S, Herbert D, Disiuta L, , et al. A Survey on Blockchain-Based Internet Service Architecture: Requirements, Challenges, Trends, and Future. *IEEE Access* . 2019;7:75845 –75872. Available from: https://doi.org/10.1109/ACCESS.2019.2917562.
11) Chauhan A, Savner G, Venkatesh P, Patil V, Wu W. A Blockchain-Based Tracking System. In: International Conference On Service Oriented Systems Engineering (Sose). IEEE. 2020;p. 111–115. Available from: https://doi.org/10.1109/SOSE49046.2020.00020.
12) Xie W, Wu W, Wang B, You J, Ye Z, Zhou Q. Simulation-Based Blockchain Design To Secure Biopharmaceutical Supply Chain. In: 2019 Winter Simulation Conference. IEEE. 2020. Available from: https://doi.org/10.1109/WSC40007.2019.9004696.
13) Dongre PB, and PV. An IOT Based Private Blockchain Framework for Attendance Management Using QR Code. In: Proceedings of the First International Conference on Advanced Scientific Innovation in Science, Engineering and Technology, ICASISET 2020. 2021;p. 1–15. Available from: https://eudl.eu/pdf/10.4108/eai.16-5-2020.2303960.
14) Van Dung Nguyen, Van Khoa H, Kieu TN, Huh EN. Internet of Things-Based Intelligent Attendance System: Framework, Practice Implementation, and Application. *Electronics* . 2022;11(19):1–19. Available from: https://doi.org/10.3390/electronics11193151.
15) Al-Khazaali AAT, Kurnaz S. Study of integration of block chain and Internet of Things (IoT): an opportunity, challenges, and applications as medical sector and healthcare. *Applied Nanoscience*. 2023;13:1531–1537. Available from: https://doi.org/10.1007/s13204-021-02070-5.
16) Sarma P, ul Isla A, Bayan T. Iot-Based Agriculture Environment And Security Monitoring System. *Periódico Tchê Química*. 2023;20(44):15–31. Available from: https://www.tchequimica.com/arquivos_jornal/2023/44/02_ATOWAR_pgs_15_31.pdf.
17) Singh AK, Kumar S. An efficient and secure CLAKA protocol for blockchain-aided wireless body area networks. *Expert Systems with Applications*. 2024;242. Available from: https://doi.org/10.1016/j.eswa.2023.122740.
18) Vaiyapuri T, Shankar K, Rajendran S, Kumar S, Acharya S. Blockchain Assisted Data Edge Verification With Consensus Algorithm for Machine Learning Assisted IoT". *IEEE Access*. 2023;11:55370–55379. Available from: https://doi.org/10.1109/ACCESS.2023.3280798.

19) Gandhi S, Kiwelekar A, Netak L, Shahare S. A blockchain-based data-driven trustworthy approval process system. *International Journal of Information Management Data Insights*. 2023;3(1):1–10. Available from: https://dx.doi.org/10.1016/j.jjimei.2023.100162.

20) Hanggoro D, Windiatmaja JH, Sari RF. Blockchain-based Attendance Management and Payroll System using Hyperledger Composer Framework. In: 2022 IEEE Region 10 Symposium (TENSYMP). IEEE. 2022. Available from: https://doi.org/10.1109/TENSYMP54529.2022.9864383.

21) Kamal ZA, Fareed R. A Proposed hash algorithm to use for blockchain base transaction flow system. *Periodicals of Engineering and Natural Sciences (PEN)*. 2021;9(4):657–673. Available from: https://dx.doi.org/10.21533/pen.v9i4.2401.

22) Khadidos AO, Khadidos AO, Selvarajan S, Mirzatasla OM. TasLA: An innovative Tasmanian and Lichtenberg optimized attention deep convolution based data fusion model for IoMT smart healthcare. *Alexandria Engineering Journal*. 2023;79:337–353. Available from: https://doi.org/10.1016/j.aej.2023.08.010.

23) Syed NF, Shah SW, Shaghaghi A, Anwar A, Baig Z, Doss R. Zero Trust Architecture (ZTA): A Comprehensive Survey. *IEEE Access*. 2022;10:57143–57179. Available from: https://doi.org/10.1109/ACCESS.2022.3174679.

24) Colombo P, Ferrari E. Access control technologies for Big Data management systems: literature review and future trends. *Cybersecurity”*. 2019;2:1–13. Available from: https://doi.org/10.1186/s42400-018-0020-9.

25) Song G, Wang Y, Li Y. Dynamic Mathematical Model of Information Spreading on News Platform. *Wireless Communications and Mobile Computing*. 2021;2021(1):1–11. Available from: https://doi.org/10.1155/2021/2174190.

26) Shitharth S, Manoharan H, Shankar A, Alsowail RA, Pandiaraj S, Edalatpanah SA, et al. Federated learning optimization: A computational blockchain process with offloading analysis to enhance security. *Egyptian Informatics Journal*. 2023;24(4):1–12. Available from: https://doi.org/10.1016/j.eij.2023.100406.

27) Aljumah A, Ahanger TA. Blockchain-Based Information Sharing Security for the Internet of Things. *Mathematics*. 2023;11(9):1–20. Available from: https://dx.doi.org/10.3390/math11092157.