Towards Implementation of IOTDMS Blockchain Framework for Secure Data Sharing Among IoT Devices

Miss. Priyanka B. Dongre[1], Dr. Pushpneel Verma[2]
[1]*Research Scholar, Bhagwant University, Ajmer, Rajasthan*
[2]*Associate Professor, Bhagwant University, Ajmer, Rajasthan*

Abstract **- In this era of digital communication lots of companies are using IoT devices to manage and store day to day transaction data. Many organizations use biometric based attendance system to mark the attendance of employees. Few organizations use RFID cards or tags embedded in identity card of employee. Smart phone has become a handy tool for people for not only communication but for transferring money from bank account and digital wallets using QR codes as a means for transaction. Similarly, blockchain has emerged as a tool to securing transactions of cryptocurrencies. Considering the advantages and disadvantages of each of these means, we have designed a novel blockchain framework called IOTDMS Chain which will help users to perform several transactions in a secured way using the IoT devices.**

Index Terms **- blockchain, IOT, RFID, security, privacy, data, IOTDMS chain, AMS.**

I.INTRODUCTION

To secure data in Internet of Things (IoT), implementation of Blockchain algorithm is becoming popular and its widespread use and applications in industries are increasing day by day and rapidly. It is believed that by 2020, Over 25 billion devices are expected to be connected to the Internet. The Internet of Things (IoT) enabled applications that offer socioeconomic benefits, because of exponentially increasing number of connected devices. A variety of IoT applications have different operational requirements and constraints.

The issues like user authentication, device identity, data security, and so on are posing limitation on implementing IoT. Security and data privacy is a significant concern in IT industry where network of computers share the data among several and different users. Depending on the application and usage, IT industry has implemented and continued to implement a variety of data privacy and security tools.

These tradition nature security solutions are not always applicable to "Internet of Things" due to many reasons like IOT contains a network of heterogeneous devices that run on varied embedded devices, operating systems, number of devices connected in IOT and so on. Unfortunately, like any other industry in IOT industry data privacy and security is often disregarded.

On the other hand, with the introduction of cryptocurrency called "Bitcoin" which is tracked securely using Blockchain technology is becoming popular and accepted worldwide. The blockchain technology has proved its potential to identify and trace each transaction irrespective location and network and helps in identification of device, secures data transfer and immutable data storage.

The aim of this research is to provide comparative analysis of blockchain frameworks and algorithms and propose an algorithm that can be employed on Internet of Things to secure the data transfer and maintain the data privacy. This research will help managers and developers to quickly review the suitable framework for their application depending upon their requirements. A case study involving a small Internet of Things consisting computers, mobile phones, embedded devices etc. will be implemented to test the algorithm or framework that is applicable to a real-world problem.

II. LITERATURE REVIEW

Ali Dorri et. al. (2017) proposed a framework to address the security, privacy, and performance of the IoT based smart home and presented the simulated results of traffic overhead & processing overhead in blockchain. It is a hierarchical architecture that

contains three tiers as Smart Home, Overlay Network and Cloud Storage. The Smart home contains several IoT devices like thermostat, smart bulbs, an IP camera, sensors etc. The authors ensured decentralized topology is maintained through methods that are distributed and trustworthy. At each tire the authors used local, shared and private Blockchain to securely access the data, control and monitor the devices in IoT smart home network. In this framework the symmetric encryption is used to maintain confidentiality, hashing technique is used to achieve integrity, logging transactions in local Blockchain ensures user control, policy holder and shared keys are used for authorization purpose. However, the authors stated that in worst case for a query-based store transaction the time overhead is 20ms and it increases the energy consumption by 0.07 (mj) of IoT devices [1], [2].

Rawia Bdiwi et. al. (2017) proposed a ubiquitous learning environment (ULE) that is implemented and secured by combing the features of IoT and Blockchain. The learning environment contained devices like IP Camera, integrated sensors, Smart TV, interactive white board, sensors and devices that collects the data and transmit it over internet for analysis and processing. These devices act as the contact point between student and teacher in the ubiquitous learning environment. The cloud-based BC platform allows students and teachers to access the data and services securely. Transaction reliability is ensured using cryptographic hashes. The authors used "consensus protocol" to verify the ledger and transaction sharing is efficient. This distributed architecture helps to decentralize the system [3].

Zhe Yang et. al. (2017) proposed reputation system that allows to judge the message received from sender based on his reputation score. The system is implanted using Blockchain technology for vehicular network. The reputation value of a sender / vehicle is calculated using the historical ratings. The building blocks of proposed systems are the entities involved and procedures. The four entities in the system are trusted authority (TA), ordinary vehicle (OV), malicious vehicle (MV), and miner. The trusted authority (TA) is responsible for registration and allocation of ID, public key and private key. TA also certifies the sensing capacity of vehicle. Ordinary Vehicles remain in vehicle cluster till it is selected by miner. These vehicles can send and receive messages, provide ratings, and can receive raging packages from miner. Malicious Vehicles may exist in the network which may try to disturb the network operation, broadcast false messages, fake ratings etc. The miner is a temporary center node elected among vehicles using specific rules. The procedure includes Data credibility assessment, Rating, Miner election, Block generation and validation, Distributed consensus, Reputation calculation. The authors claimed that the system is able to improve the security of vehicular networks after conducting number of experiments for verifying the reliability of system [4].

Jung, M. Y., & Jang, J. W. (2017), used ECDSA digital signature and SHA-256 hash function in Blockchain to ensure security in data management and data searching system for IoT network. The authors used security properties of Blockchain includes authentication, non-repudiation and data integrity. The Blockchain contains the IP address and data name of the owner. Block hash value is analyzed to implement data management and searching. Based on the simulation results the authors claims that the system is able to prevent IP spoofing, Sybil attack and single point failure. The system is easy to manage [5].

Tian, F. (2017, June) discussed general challenges in scaling blockchains and proposed a decentralized traceability system employing IoT & Blockchain. The author explained the working of proposed system with an example scenario of food supply chain based on Hazard Analysis and Critical Control Points. The theoretical and application concept proposed by author may improve the efficiency and transparency in supply chain as well provide real time information to gain the consumer's confidence in the food industry [6].

Han, D., Kim, H., & Jang, J. (2017) implemented a Smart Door Lock system based on Blockchain using CPU, TCP/IP, Bluetooth / Zigbee, GPS and sensors. The system is able to identify the unauthorized access, inside and outside intruders, immediately. The system also implements security features like non-repudiation and data integrity implemented through proof of work. The first receiver block is added to chain when miner completes (n+1) rounds and all nodes creates and broadcasts (n+1) blocks. Authors also suggest that 3 to 4 zero bits are required to establish a real-time blockchain network [7].

Xie, C., Sun, Y., & Luo, H. (2017) proposed a three-layer scheme for storing tracking data of agriculture products using Blockchain technology. The sensing layer is the internet of things comprising several

sensors like temperature, humidity, pressure, acceleration, GPS and GPRS modules. These IoT devices write the data-to-Data Storage Layer when a certain action is sensed by sensors. The double chain data storage system is implemented in Ethereum blockchain framework. The system automatically performs encapsulation and data analysis on the data received from sensors and writes it to blockchain. To secure the database transaction hash is used and for improving I/O data efficiency auxiliary database is used. Application Layer enables the user to access data system services through specific applications designed for the specific service [8].

To manage the privacy preference in IoT network Shi-Cho Cha et. al. (2017) proposed the design of a Blockchain based connected Gateway called BC Gateway. To explain the functionality of BC Gateway authors used three types of participant. The first participant is the either owner of IoT Device or Administrator of IoT Device. The second participant is the administrator of BC Gateway and third is the end user. In this system the user can access the IoT device through BC Gateway by obtaining the device information and accepting the privacy policy and the preference is stored on Blockchain network. To resolve the disputes between IoT service provider and user the user preference data can be utilized. Every IoT device is registered on BC Gateway through a device binding where device manager stores the device information and privacy policies using smart contracts. The authors conducted experiment on Etherum network by simulating the BC Gateway and client application on android mobile phone. To implement security features authors used Raspberry PI III Model B for implementing a six "Setup", "Set-Partial-Private-Key", "Set-Secret-Value", "Set-Public-Key", "Sign" and "Verify" phase Digital Signature Scheme. The computational cost of each security module is obtained as shown below [9].

Table 1: Computational cost of security module [9]

Security Module	Cost
Random number generator (96 bits)	0.5ms
Hash function (SHA-512 with input 1000 bits)	7ms
ECC Pairing (384 bits)	240ms
ECC point multiplication (384 bits)	4ms
ECC point addition (384 bits)	2ms

Ozymaz, K. R., & Yurdakul, A. (2017) configured IoT Gateway in a private etherum network using LoRa nodes as blockchain node for low power IoT devices. As the low power IoT devices can not afford to run complex and long duration blockchain calculations the authors implemented event-based messaging mechanism. End device and a Gateway is implemented using LoRa with Raspberry Pi2 and Pi 3 connected to Dragino LoRa/GPS Hat and iC880A from IMST. A smart contract termed as "Bridge" having two events and two functions enables the communication between end devices and gateway. The two events process and notify whereas the functions are request and activate [10].

Zhu, X., Badr, Y., Pacheco, J., & Hariri, S. (2017) introduced a method for extracting unique signatures which uniquely identifies each IoT device used in Smart Homes. The authors also proposed a distributed and trustworthy Identity Management System based on Blockchain Identity Framework (BIFIT). The system implements two phase, first training the system offline and the second test the system online. Using this method user can monitor and control the various sensors embedded with the appliances like LED Light, AC Lamp, Ventilator, Door Lock, Television etc. [11].

Ning Zhou, Menghan Wu, and Jianxin Zhou (2017), presented a study that utilizes blockchain technology and internet of things to record, store and secure the volunteer service time so that the volunteer's personal data remain secure using smart contracts of blockchain and they are rewarded to keep them motivated for volunteering [12].

Zheng. Z. et. al (2017) explained the overview of Blockchain architecture, its characteristics, consensus algorithms and its comparison in detail along with few challenges and suggestions for future work. The table below describes the comparison among public, consortium and private blockchain [13].

Table 2: Comparison among public, consortium and private blockchain

Property	Public blockchain	Consortium blockchain	Private blockchain
Consensus determination	All miners	Selected set of nodes	One organization
Read Permission	Public	Public or Restricted	Public or Restricted
Immutability	Impossible to tamper	Can be tampered	Can be tampered
Efficiency	Low	High	High
Centralized	No	Partial	Yes
Consensus process	Permission less	Requires permission	Requires permission

The table below shows the comparison among consensus algorithms [13].

Table 3: Comparison among consensus algorithms

Property	PoW	PoS	PBFT	DPOS	Ripple	Tendermint
Node Identity Management	Open	Open	Permissioned	Open	Open	Permissioned
Energy Saving	No	Partial	Yes	Partial	Yes	Yes
Tolerated power of adversary	<25% Computing power	<51% stakes	<33% faulty replicas	<51% Validators	<20% faulty nodes	<33% byzantine voting power
Example	Bitcoin	Peercoin	Hyperledger Fabric	Bitshares	Ripple	Tenermint

Pradip Kumar Sharma, Mu-Yen Chen, and Jong Hyuk Park (2017) proposed an architecture based on fog computing, software defined networking (SDN) and blockchain to address the issues in IoT network like availability, data delivery in real time, security, scalability, latency and resiliency. IoT devices generate the raw data streams in distributed cloud and at the edge of IoT network considering this things authors designed a new distributed cloud architecture based on blockchain. As compared with traditional IoT network the authors model reduces traffic load, computing resources and end to end delay among devices in the distributed blockchain cloud network. The authors evaluated the model on several parameters like throughput, response time, delay-incurred performance metrics, accuracy rate of attack detection and presence of different traffic [14].

Zonyin Shae and Jeffrey J. P. Tsai (2017) discussed design aspects, technology requirements and challenges for a blockchain based architecture aimed to analyze clinical trial and precision medicine data using big data analytics and IoT. The authors identified four different components and discussed requirements and challenges for implementation in the proposed architecture [15]. The four components are listed below.

1. Distributed and parallel computing based on blockchain to devise and study parallel computing methodology for big data analytics.
2. blockchain application data management component for data integrity, big data integration, and integrating disparity of medical related data,
3. verifiable anonymous identity management component for identity privacy for both person and Internet of Things (IoT) devices and secure data access to make possible of the patient centric medicine, and
4. trust data sharing management component to enable a trust medical data ecosystem for collaborative research [15].

According to Salahuddin, M. A. et. al. (2017) IoT networks has a potential to be applied in implementing smart health care solutions as the IoT devices has ability to generate large amount of data in the form of text, audio and video. To utilize this data in health care we will require an effective mechanism for collecting, aggregating, batch processing and pseudo-real or real time processing as the data comes from heterogeneous sources on IoT network. To overcome these issues the authors proposed a cost effective, flexible and secure software architecture build using cloud computing, fog computing and blockchain that can be employed in private IoT for smart health care applications. The architecture provides features such as machine to machine (M2M) messaging, rule base for data management, data and decision fusion so that the smart health care applications and services can be used effectively [16].

Rifi, N., Rachkidi, E., Agoulmine, N., & Taher, N. C. (2017) has proposed a method to secure IoT network using Publisher Subscriber data sharing mechanism with blockchain technology. The method is based on smart contracts between provider and a consumer. The authors used off chain database technology to deal with data storage problems. The block stores the information of contract and reference to where the data is stored. To study the mining process performance with respect to overall system response time the authors presented a data analytic model. A decentralized applications (DApps) framework called Embark is used with Etherum blockchain, IPFS database and Whisper protocol to exchange messages between applications. The authors implemented their private blockchain with two gateways implemented on Raspberry Pi & laptop and a go etherum (geth) client,

that notifies when the new smart contract is generated or updated. The smarts contracts are implemented using SolidityC programming whereas the frontend and GUI is implemented using HTML, Javascript and JQuery [17].

Pinno, O. J. A., Gregio, A. R. A., & De Bona, L. C. (2017) proposed an architecture called "ControlChain" which is decentralized, resilience, and capable of working offline to control and authorize access in IoT network. The ControlChain is different from traditional architectures in the sense that it is a completely decentralized and provides transparency in authorization process also it compatible with other access control models used in IoT. The architecture provides a secure way to create relationships, assign attributes and use them in access control. According to authors the traditional access control architectures XACML, OAuth, UMA and FairAccess are unable to provide the full stack of features as compare to ControlChain. The authors presented a comparison as shown in table below [18].

Table 4: Architecture Comparison

Architecture → / Features ↓	XACML	OAuth	UMA	FairAccess	Control Chain
Scalability	-	-	-	+	+
Fault Tolerant	-	-	-	+-	+
No third parties	-	-	-	+	+
New authorization	+	+	+	-	-(*)
Get authorization	+	+	+	-(*)	+
Integr. Relationship	-	-	-	-	+
Compatibility	+	-	-	-	+
Low object overhead	+	+	+	+	+

(*) dependent on the type of proof and dissemination speed of blocks [18].

Park, J., & Kim, K. (2017) presented a model called "TM-Coin" for trustworthy, efficient remote attestation and decentralized management of Trusted Computing Base (TCB) in IoT devices based on blockchain technology. TM-Coin has taken maximum advantage of ARM TrustZone and blockchain to securely manage the TCB measurement of IoT devices. It implements miners and verifiers to remotely attest the data received from IoT devices that use TCB measurement method and publish them in Blockchain. The authors implemented the prototype using ARM TrustZone based development board [19].

Considering the potential of drones to be used in future IoT applications, Liang, X., Zhao, J., Shetty, S., & Li, D. (2017) has designed a general architecture using blockchain. The architecture aims to methods for identifying "Trusted Data Origin", "Instant and Permanent Data Integrity", "Trusted Accountability" and "Resilient Backend" while employing drone as an IoT device. The architecture contains important system elements as "Drone", "Control System", "Blockchain Network", "Cloud Database", and "Cloud Server". The authors claim that the system is reliable and accountable for real time data collection and drone control and at the same time it reduces potential attacks and data losses [20].

Li, C., & Zhang, L. J. (2017) presented a model that employs blockchain technology using wide area networking in IoT. The basic idea is to divide the IoT network in decentralized multiple levels and implement the blockchain across each level to ensure the security. The authors enlisted four advantages of using this model are 1) Using a centralized local instrument to coordinate with other IoT devices ensures safety. 2) Computational load, network load and concentrated risks are reducing with the presence of multiple centers. 3) Peer-to-peer communication is established between centers. 4) Contracts record in multiple blockchains ensure secure and reliable IoT network. Authors mention that the total cost of network may increases due to decentralization and additional resources also longer processing time is required to maintain contracts [21].

Ao Lei et. al. (2017) proposed a method that works with heterogeneous networks for secure key management. The authors presented a novel network topology for vehicular communication systems(VCS) based on blockchain to simplify the distributed key management in VCS. The security managers (SMs) captures the vehicle information, encapsulates the block to issue keys, and executes the rekeys to vehicles present in the same security domain. The framework utilizes dynamic transaction collection period to reduce timing of key transfer and handover to other vehicles. The authors presented a simulation of the proposed framework [22].

Huang Z. et. al. (2017) presented an analysis of requirements for data exchange in IoT network. From the security perspective the data exchange must meet

three major requirements i.e. trusted privacy preserving policies, trusted access to data and trusted trading. The authors developed a prototype using Etherum blockchain for data exchange in IoT. The prototype includes 10 Etherum nodes as a Blockchain network on an Ubuntu system. Out of these two nodes are used for mining and are deployed in Aliyun servers while others are utilized for IoT data exchange using PC. SolidiyC is used to implement smart contracts which are compiled on any of the miner nodes [23].

Urien, P. (2018) has discussed about integrating secure elements for the blockchain transaction processing in a trusted way. The author also planned to develop Blockchain IoT platform leverage the blockchain technology. According to author the blockchain transaction processing based on ECDSA signature is prone to attack and can be stolen. To eliminate this risk author suggested to use javacard secured elements [24].

Christidis, K., & Devetsikiotis, M. (2016) has examined the fitness of blockchain in the field of Internet of things. The authors reviewed the working mechanism of blockchain and explored the whether its combination with IoT is helpful in creation of the market in which services of devices, and resources can be shared through a cryptographically secured and automated mechanism. The authors also identified and discussed several implantation issues of these technology and concluded that the combination of blockchain and IoT will definitely contribute in introducing the new business models and distributed applications [25].

Nir Kshetri (2017) has mentioned in [26] that based on the evolving mechanisms a promising future seems likely for the use of blockchain in addressing IoT security. For instance, some of the key security challenges associated with the cloud can be addressed by using the decentralized, autonomous, and trusted capabilities of blockchain. Blockchain's decentralized and consensus-driven structures are likely to provide more secure approaches as the network size increases exponentially. Blockchain enables the verification of the attributes it carries. Blockchain-based transactions are easily auditable. Due primarily to this and other features, blockchain can play a key role in tracking the sources of insecurity in supply chains as well as in handling and dealing with crisis situations such as product recalls that occur after safety and security vulnerabilities are found. And as mentioned, blockchain-based identity and access management systems can address key IoT security challenges such as those associated with IP spoofing [26].

Thomas Lundqvist, Andreas de Blanche, H. Robert H. Andersson (2017) presented a proof-of-concept to allow one "thing" to pay another "thing" for the electricity it consumes. The authors have presented a single-fee micropayment protocol that aggregates multiple smaller payments incrementally into one larger transaction needing only one transaction fee. This protocol addresses high transaction fees problems for microtransactions in Bitcoin network [27].

In order to address these privacy issues, Yogachandran Rahulamathavan, Raphael C.-W Phan, Muttukrishnan Rajarajan, Sudip Misra, and Ahmet Kondoz (2017) proposed a new privacy-preserving blockchain architecture for IoT applications based on attribute-based encryption (ABE) techniques. Security, privacy, and numerical analyses are presented to validate the proposed model. The numerical analysis section showed that the blockchain-powered IoT can benefit from attribute-based encryption in terms of achieving privacy for minimal computational overhead [28].

To make things autonomous Mayra Samaniego, Ralph Deters (2017) has presented a hybrid framework IoST (internet of smart things) using Blockchain and CLIPS in [29]. The results of the evaluations showed that hybrid solutions are a good option to enable autonomous features in IoT networks. The resources of the Smart Things demonstrated a satisfactory performance analyzing and inferring knowledge from every data received [29].

Matevz Pustisek Andrej Kos (2017) has presented approaches to front end IOT application development for the Ethereum blockchain. The authors are currently developing tools to generate and monitor transactions in the IoT devices automatically, which will enable a systematic performance testing of the abovementioned architectures [30].

Kazim Rifat Ozyilmaz Arda Yadrakul (2017) has presented a proof of concept to enable low-power, resource-constrained IoT end-devices accessing a blockchain-based infrastructure. To achieve this aim, an IoT gateway is configured as a blockchain node and an event-based messaging mechanism for low-power IoT end-devices is proposed. A demonstration of such a system is realized using LoRa nodes and gateway in a private Ethereum network [31].

Shitang Yu, Zhou Shao, Yingcheng Guo, Jun Zou, Bo Zhang (2018) has proposed a design of a high performance blockchain platform for intelligent devices. The platform achieves efficient connection of intelligent devices through the node-to-node mapping mechanism of intelligent devices. At the same time, the authors design a blockchain consensus algorithm for intelligent devices, which provides higher consensus efficiency while guarantee the decentralization, provide higher efficiency. This system can make all the relevant parties of the intelligent devices obtain higher efficiency and benefits and achieve a result of multi-win [32].

Ying Liu, Kai Zheng, Paul Craig, Yuexuan Li, Yangkai Luo, Xin Huang (2018) has demonstrated the utility of continuous-time Markov chain (CTMC) model and continuous stochastic logic (CSL) to evaluate the reliability of a blockchain based IoT application. Experimental results show that decreasing the number of end and edge devices and decreasing the failure rate of peers will increase the reliability with the number of devices being the principle factor affecting reliability [33].

Fangmin Xu, Fan Yang, Chenglin Zhao, Chao Fang (2018) has introduced an architecture of edge computing based blockchain network which makes use of the computation and caching capacity of edge server to help the IoT devices in reaching consensus and storing data. The architecture could not only make consensus and store the data, but also could have high throughput by introducing edge computing [34].

III. OVERVIEW OF PROPOSED SYSTEM

The proposed system implements three different modules. All the three modules are integrated to show the working of IoT and blockchain for data transfer, communication. The blockchain is the core of the system. The prime goal is to create a new blockchain framework that will capture data from various IoT devices and will store it on blockchain.

This decentralized platform is mainly intended to be used by the academic institutions or universities in which the obsolete attendance system will be replaced with the new blockchain based attendance system. Using the web interface users can operate all the provided functionality. However, this web interface is one of the parts of a larger system.

As shown in the figure 4.1, to use product, users are required to register through the web interface. All the user only related to that particular organization and have the unique identity in the organization can be the part of the system. The user will be provided with the account which he/she will use to mark the attendance as the student or if he/she is a teacher then he will generate daily QR code for the students to mark the attendance for a subject at particular time. Another option to mark the attendance is using RFID cards or RFID tags. The teacher will pull the RFID data into the blockchain. Other user such as the dean of the department or the director of the college will have the view access to all these occurring scenarios and they will be able to analyze the data accordingly.

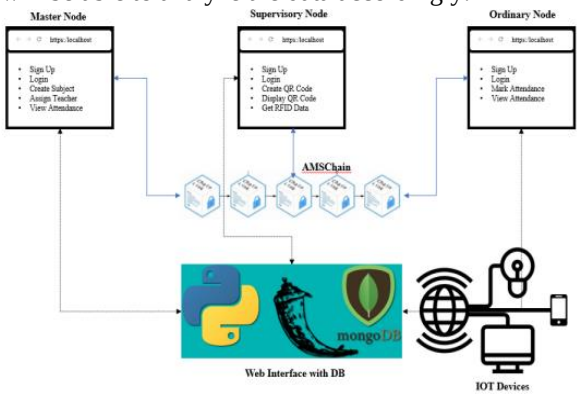

Fig. 3.1 System Architecture

IV. IMPLEMENTATION OF WEB INTERFACE

The web interface is implemented using Python, Flask and JavaScript. The web application is a distributed, multitier system with a client and a server. MongoDB is used to store the transaction records. The system is divided into following parts:

4.1.1 Client Implementation

The client side of the application is implemented in HTML, CSS, JavaScript using Python and Flask web development framework. The Client contains a home page on which interface for signup and login are provided. All of the pages make Every node having capability to access web interface send the HTTP request to server running on the middle tier, which fetches data from the Blockchain or the database and displays on the user interface. Data can also be created on the blockchain or the database by using forms that are used when the signup to the application, marking attendance, creating subjects, assigning new teachers and so on.

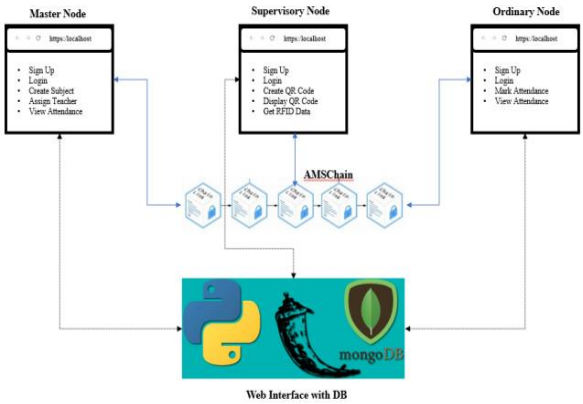

Fig. 4.1 Web Interface with DB and Blockchain

4.1.2 Middle-Tier Implementation

Middle tier is a python flask based local host server that provides web interface known as API's to all connected nodes which perform various transactions on the blockchain and MongoDB database server. Some of the API's are user signup, user login etc.

4.1.3 Data-Tier Implementation

There are two components in the data tier, IOTDMS Chain and MongoDB. Design decision has been made to store the user details data on to the MongoDB server, and it also acts as a backup server to store the blockchain data. Each transaction performed is added to the block and stored on the IOTDMS Chain by writing smart contracts for all the relevant data structures.

4.1.4 Role Based Access Control Implementation

Role based access control (RBAC) is an approach to restricting an application access based on user roles (student-ordinary node, teacher-supervisory node and dean-master node). The data communication and data sharing logic of this decentralized application is driven by smart contracts. These smart contracts are coded in Python, which is an object oriented and high-level programming language. Typically, roles reflect the permissions needed to access the web-based application. The system ensures that all the parties act honestly. Each of these users performs various transactions.

V. IMPLEMENTATION OF IOTDMSCHAIN

The proposed blockchain is implemented in python and named as IOTDMS chain. IOTDMS chain is the core of the proposed system. The main objective was to get the data from the devices connected in a IoT network and store the data on the blockchain. In IOTDMS Chain all transactions are stored as the user performs it. As the IoT devices have limitations such as less or no storage memory, less computing power the blockchain data is stored on MongoDB server for future reference. The proposed IOTDMS Chain is based on SHA256 and asymmetric encryption algorithm RSA. Figure 4.3 shows the IOTDMS chain infrastructure implemented in four layers.

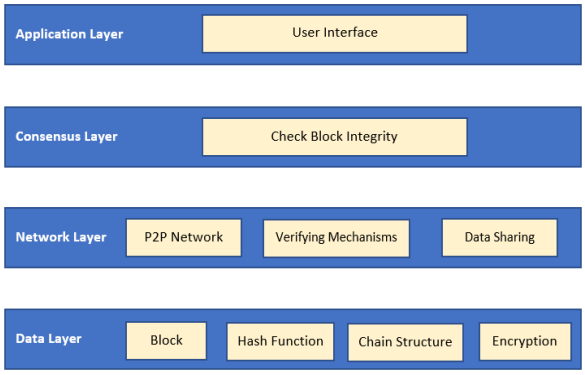

Fig. 4.3 IOTDMS Chain

The various blocks and the block data structure is discussed in subsequent section. Each block in the blockchain has the following data structure to store the transactions.

5.1.1 Block Structure

Each block stores the data entered or generated by user. The block structure is given below. The data generated by user is called a record or transaction, which is added to the block and then the block is added to the blockchain.

Block {Index: Number,
Hash: String,
Timestamp: datetime
Data: Record Structure
Previous_Hash: String
}

5.1.2 Genesis Block

Genesis Block is the first block in the blockchain and this block gets created when the code is executed for first time. As shown in figure 1.5 the genesis blocks get created and stored at index 0 in the blockchain. Later on, the other blocks are created and are added into the IOTDMS Chain. The function

create_generate_genesisblock() creates the genesis block.

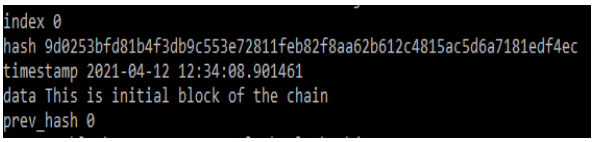

Fig. 4.4 Genesis block

5.1.3 Record / Transaction Data Structure

The data generated by each user during the use of system is added to the block as a transaction or record. Each user generates several types of records based on the user role. The record data is one of the filed in the block. Each of these records or transactions have different data structures. Some of the important record structure used in the system are discussed below.

5.1.3.1 Registration

Registration data is stored for each user or node. All the nodes have to register first to use the system during registration user has to provide the data and this data is added to the block and block is added to the blockchain. The data structure for registration data is given below.

Registration {user: String,
Email: String,
Name: String,
Password: String
}

5.1.3.2 New Subject Creation

The master node creates new subject and assign the supervisory node to the created subject. The new subject creation record or transaction has the following data structure.

New Subject {Subject Name: String,
Subject Code: String,
Department Name: String,
Class ID: String,
Number of students: int
}

5.1.3.3 Assign Teacher

The master nodes assign the subjects to teacher (supervisory node). The record is generated when the master node assigns a subject to a supervisory node. The data structure for this transaction is given below.

Assign Teacher {Department Name: String,
Class Name: String,
Subject Name: String,
Teacher Name:String
}

5.1.3.4 QR Code Generation

This transaction contains the information like name of the department, class name, class ID, number of students, subject name, subject ID, lecture starting time and lecture end time. The supervisory node generates the QR code and displays it for ordinary to mark attendance.

QR Code {Department Name: String,
Class ID: String,
Subject Name: String,
Lecture Start Time: time,
Lecture End Time: time

VI. IOT DEVICES

The IOT devices included Raspberry Pi, RFID Reader, RFID Card and RFID tags. The details of the hardware and software required to build the IOT network are discussed below. The below figure shows the actual IOT network connected. The data generated through IoT network is shared to server and uploaded to the BIOTChain. The data structure for RFID attendance record is given below.

RFID Data {Name: String,
Department Name: String,
Class Name: String,
Roll Number: Int
}

Fig. 4.6 Raspberry Pi and RFID Reader

6.1.1 Hardware

The hardware components used to build the IOT network are listed below.

- RJ45 LAN cable
- SD card and Adapter
- Raspberry pi 3 B+
- Breadboard
- RFID reader and RFID Tag/card

6.1.2 Software

The software components used to build the IOT network are listed below.

- SD card formatter
- BalenaEtcher
- VNC viewer
- PuTTY

6.1.3 Steps to connect Raspberry pi to laptop

Below are the steps to connect the Raspberry Pi to a Laptop.

- Open any browser and go to raspberrypi.org and download OS
- Insert a SD card into adapter and plug it into your laptop.
- Open SD card formatter and format your SD card.
- Open balenaEtcher and then select your OS image file.
- Then select target location and click in flash.
- Create an empty file named ssh without any extension in boot partition. It automatically enables SSH on boot and then deletes it.
- Remove SD card and insert it into your Raspberry pi.
- Then connect LAN cable from laptop to raspberry. Power it up using USB cable.
- Enter the command 'ipconfig' to configure raspberry. Under interfaces enable VNC to share screen.
- Login with username as 'pi' and password as 'raspberry'.
- Enter the command 'sudo raspi-config' to configure raspberry pi. Under interfacing options enable VNC for screen share.
- Click on system options -bool/auto login select boot into desktop or to command line -desktop auto login desktop GUI, automatically logged in as 'pi' user- click on finish.
- Open VNC viewer. Under server address type 'raspberry.local'
- Then login into the device using 'pi' as user name and 'raspberry' as password.
- Configure your raspberry pi by enter the details of your location. This id used to set the language, time zone, keyboard and other international settings.

6.1.4 Steps to setup a raspberry pi to RFID RC522 chip

Perform the following steps

- Insert the RC522 RFID module into the breadboard
- Place a wire between the 3v3 pin on the RC522 and pin 1 (3v3) on the raspberry pi.
- Place a wire between the RST pin on the RC522 and Pin 22(GPIO 22) on the Raspberry pi.
- Place a wire between the GND pin on the RC522 and Pin 6(Ground) on the Raspberry pi.
- Place a wire between the MISO pin on the RC522 and Pin 21 (MISO) on the raspberry pi.
- Place a wire between the MOSI pin on the RC522 and Pin 19 (MOSI) on the raspberry pi.
- Place a wire between the SCK pin on the RC522 and Pin 23(SCK) on the raspberry pi.
- Place a wire between the SDA pin on the RC522 and Pin 24 (SDA) on the raspberry pi.
- Start the raspi configuration tool execute a command 'sudo raspi-config'
- Select '5 Interfacing Options'
- Now choose 'P4 SPI'
- Select 'Yes' to enable the SPI interface
- Restart your Raspberry Pi using 'sudo reboot' command
- Retrieve a list of active kernel mods using 'lsmod | grep spi' command
- If 'spi_bcm2835' appears then the SPI has interface has been successfully setup.
- Update the package list using 'sudo apt-get update' command.
- Now upgrade all available packages using 'sudo apt-get upgrade' command.
- Install the 'python3-dev' and 'python3-pip' packages using 'sudo apt-get install python3-dev python3-pip' command.
- Install the spidev python3 package using 'sudo pip3 install spidev' command.
- Now install the mfrc522 library using 'sudo pip3 install mfrc522' command.

- Create a directory to store our example scripts using 'mkdir ~/pi-rfid' command.
- Change the newly created directory using 'cd ~/pi-rfid' command
- Now create the RFID write.py script using 'sudo nano write.py' command
- Write the code to take user input to the RFID card.
- Now run the script we just wrote 'sudo python3 write.py' command.
- Type in the data you want to write to your RFID card.
- Tap your RFID tag to write data to it.
- Being writing the RFID read.py script using 'sudo nano read.py' command.
- Write the code to read data from an RFID Card.
- Run the newly created read.py script using 'sudo python3 read.py' command.
- Tap your RFID tag to read data from it.

VII. CONCLUSION

This paper proposed a secure blockchain framework for data sharing among IoT Devices called "IOTDMS Chain". The proposed novel four-layer blockchain framework is under construction. We are able to generate different transactions and transaction blocks which can be added to the blockchain.

REFERENCES

[1] Dorri, A., Kanhere, S. S., & Jurdak, R. (2017, April). Towards an optimized blockchain for IoT. In Proceedings of the Second International Conference on Internet-of-Things Design and Implementation (pp. 173-178). ACM.

[2] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on (pp. 618-623). IEEE.

[3] Bdiwi, R., de Runz, C., Faiz, S., & Cherif, A. A. (2017, July). Towards a New Ubiquitous Learning Environment Based on Blockchain Technology. In Advanced Learning Technologies (ICALT), 2017 IEEE 17th International Conference on (pp. 101-102). IEEE.

[4] Yang, Z., Zheng, K., Yang, K., & Leung, V. C. (2017, October). A blockchain-based reputation system for data credibility assessment in vehicular networks. In Personal, Indoor, and Mobile Radio Communications (PIMRC), 2017 IEEE 28th Annual International Symposium on (pp. 1-5). IEEE.

[5] Jung, M. Y., & Jang, J. W. (2017, October). Data management and searching system and method to provide increased security for IoT platform". In Information and Communication Technology Convergence (ICTC), 2017 International Conference on (pp. 873-878). IEEE.

[6] Tian, F. (2017, June). A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things. In Service Systems and Service Management (ICSSSM), 2017 International Conference on (pp. 1-6). IEEE.

[7] Han, D., Kim, H., & Jang, J. (2017, October). Blockchain based smart door lock system. In Information and Communication Technology Convergence (ICTC), 2017 International Conference on (pp. 1165-1167). IEEE.

[8] Xie, C., Sun, Y., & Luo, H. (2017, August). Secured Data Storage Scheme Based on Block Chain for Agricultural Products Tracking. In Big Data Computing and Communications (BIGCOM), 2017 3rd International Conference on (pp. 45-50). IEEE.

[9] Cha, S. C., Chen, J. F., Su, C., & Yeh, K. H. (2018). A Blockchain Connected Gateway for BLE-based Devices on the Internet of Things. IEEE Access.

[10] Özyılmaz, K. R., & Yurdakul, A. (2017, October). Integrating low-power IoT devices to a blockchain-based infrastructure: work-in-progress. In Proceedings of the Thirteenth ACM International Conference on Embedded Software 2017 Companion (p. 13). ACM.

[11] Zhu, X., Badr, Y., Pacheco, J., & Hariri, S. (2017, September). Autonomic Identity Framework for the Internet of Things. In Cloud and Autonomic Computing (ICCAC), 2017 International Conference on (pp. 69-79). IEEE.

[12] Zhou, N., Wu, M., & Zhou, J. Volunteer Service Time Record System Based on Blockchain Technology. (2017). IEEE.

[13] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In Big Data (BigData Congress), 2017 IEEE International Congress on (pp. 557-564). IEEE.

[14] Sharma, P. K., Chen, M. Y., & Park, J. H. (2018). A software defined fog node based distributed blockchain cloud architecture for iot. IEEE Access, 6, 115-124.

[15] Shae, Z., & Tsai, J. J. (2017, June). On the Design of a Blockchain Platform for Clinical Trial and Precision Medicine. In Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on (pp. 1972-1980). IEEE.

[16] Salahuddin, M. A., Al-Fuqaha, A., Guizani, M., Shuaib, K., & Sallabi, F. (2017). Softwarization of Internet ofThings Infrastructure for Secureand Smart Healthcare. Computer, 50(7), 74-79.

[17] Rifi, N., Rachkidi, E., Agoulmine, N., & Taher, N. C. (2017, September). Towards using blockchain technology for IoT data access protection. In Ubiquitous Wireless Broadband (ICUWB), 2017 IEEE 17th International Conference on (pp. 1-5). IEEE.

[18] Pinno, O. J. A., Gregio, A. R. A., & De Bona, L. C. (2017, December). ControlChain: Blockchain as a Central Enabler for Access Control Authorizations in the IoT. In GLOBECOM 2017-2017 IEEE Global Communications Conference (pp. 1-6). IEEE.

[19] Park, J., & Kim, K. (2017, March). TM-Coin: Trustworthy management of TCB measurements in IoT. In Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on (pp. 654-659). IEEE.

[20] Liang, X., Zhao, J., Shetty, S., & Li, D. (2017, October). Towards data assurance and resilience in IoT using blockchain. In Military Communications Conference (MILCOM), MILCOM 2017-2017 IEEE (pp. 261-266). IEEE.

[21] Li, C., & Zhang, L. J. (2017, June). A Blockchain Based New Secure Multi-Layer Network Model for Internet of Things. In Internet of Things (ICIOT), 2017 IEEE International Congress on (pp. 33-41). IEEE.

[22] Lei, A., Cruickshank, H., Cao, Y., Asuquo, P., Ogah, C. P. A., & Sun, Z. (2017). Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. IEEE Internet of Things Journal, 4(6), 1832-1843.

[23] Huang, Z., Su, X., Zhang, Y., Shi, C., Zhang, H., & Xie, L. (2017, December). A decentralized solution for IoT data trusted exchange based-on blockchain. In Computer and Communications (ICCC), 2017 3rd IEEE International Conference on (pp. 1180-1184). IEEE.

[24] Urien, P. (2018, February). Towards secure elements for trusted transactions in blockchain and blockchain IoT (BIoT) Platforms. Invited paper. In Mobile and Secure Services (MobiSecServ), 2018 Fourth International Conference on (pp. 1-5). IEEE.

[25] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. IEEE Access, 4, 2292-2303.

[26] Kshetri, N. (2017). Can blockchain strengthen the internet of things? IT professional, 19(4), 68-72.

[27] Lundqvist, T., De Blanche, A., & Andersson, H. R. H. (2017, June). Thing-to-thing electricity micro payments using blockchain technology. In 2017 Global Internet of Things Summit (GIoTS) (pp. 1-6). IEEE.

[28] Rahulamathavan, Y., Phan, R. C. W., Rajarajan, M., Misra, S., & Kondoz, A. (2017, December). Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption. In 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS) (pp. 1-6). IEEE.

[29] Samaniego, M., & Deters, R. (2017, June). Internet of smart things-IoST: using blockchain and clips to make things autonomous. In 2017 IEEE international conference on cognitive computing (ICCC) (pp. 9-16). IEEE.

[30] Pustisek, M., & Kos, A. (2018). Approaches to front-end IOT application development for the Ethereum blockchain. Procedia Computer Science, 129, 410-419.

[31] Ozyilmaz, K. R., & Yurdakul, A. (2017, October). Integrating low-power IoT devices to a blockchain-based infrastructure: work-in-progress. In Proceedings of the Thirteenth ACM International Conference on Embedded Software 2017 Companion (p. 13). ACM.

[32] Yu, S., Lv, K., Shao, Z., Guo, Y., Zou, J., & Zhang, B. (2018, August). A high performance blockchain platform for intelligent devices. In 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN) (pp. 260-261). IEEE.

[33] Liu, Y., Zheng, K., Craig, P., Li, Y., Luo, Y., & Huang, X. (2018, August). Evaluating the Reliability of Blockchain Based Internet of Things Applications. In 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN) (pp. 230-231). IEEE.

[34] Xu, F., Yang, F., Zhao, C., & Fang, C. (2018, August). Edge Computing and Caching based Blockchain IoT Network. In 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN) (pp. 238-239). IEEE.

[35] Lee, C., Sung, N. M., Nkenyereye, L., & Song, J. (2018). Demo Abstract: Blockchain enabled Internet-of-Things Service Platform for Industrial Domain. In 2018 IEEE International Conference on Industrial Internet (ICII) (No. 595).