Block-Chain Based Authentication Technique

Pratiksha P. Gofane, Vijay S. Gulhane, Harshal N. Datir

Abstract*: *The Block-chain technology contain multiple blocks are interconnected to each other with help of previous hash and current hash. The Block-chain is technology which is used to enable for moving some coin, data and assets from one user to another user. Where using hash algorithm, cryptographic algorithm and block-chain maintenance/updating. Block-chain technology contain the previous hash of first block is always zero that is called genesis block and current block will generate according to the data. In block-chain technology after complete the first block system automatically generated new block. Second block contain the previous hash will be always current hash of first block for interconnect the blocks and chain will formed ahead. According to this chain automatically detect there some transparency and this transparency says that block chain is very secured technology. This block-chain technology with transaction is very safe for companies, colleges and business. It is layered framework technology. Where perception layer, transmission layer, storage layer and application layer are present. In block-chain technology transaction contain there need not any third trusted party. Previous concept of block-chain with IOT that is not secured where some disadvantages of limited storage present and reduce that limitation we are using distributed ledger of block-chain technology. Where system have occurred peer to peer transaction. Further, block-chain contain well organized their weaknesses, strengths, opportunities, and threats of block-chain based transaction application. In block-chain contain using with OTP this block-chain will be more secured and easily transfer the money. Their future scope in business, education and companies.

Keywords*: *Block-chain, Block-chain types, Block-chain requirements & Block-chain security process.

I. INTRODUCTION

The block-chain based authentication technology refers to the securing IOTs in distributed block-chain analysis, requirements and open issues [1]. The block-chain is technology that enables for moving data, assets and digital coin from one end to another end. It is used in a crypto currency. The block-chain contains the transfer crypto currency without any third trusted party. It is immediately transfer the money. It is discovered in 1991 but that time not exposure this technology. Until 2008 Satoshi Nakamoto launched bit-coin with help of block-chain

Technology. The block-chain technology contain we are used distributed ledger. In this distributed ledger contain the peer to peer transaction occurred. In block-chain technology with transaction there are two principle is open ledger and distributed ledger. Open ledger Fig.2 it is called centralized ledger. Distributed ledger Fig.3 it is called decentralized ledger. There is both principle of same value [2]. Suppose open ledger contain the four peoples are present. That time every people knows all details about every people because this is open ledger and open ledger it is centralized ledger. In block-chain contain distributed ledger of a peer to peer transaction where only sender user and receiver user transmit the data [3].

This block-chain are categorized in three section [4]. That section is public block-chain, private block-chain and consortium block-chain. In this block-chain we will use any type of block-chain. But there are some rules and regulation are present in block-chain. Where block-chain contain the every section is trusted section. Some authority are present there. Every user need to follow some instruction. Where need to verify the each user. In Fig.1 block-chain technology contain every block has data, previous hash and current hash are present. In which data means some like transactional record. Previous hash of first block is always zero that is called genesis block and Current hash is generate according data. After complete the first block system automatically generate the new block. This new block contain the previous hash is always current hash of a previous block and current hash is generate according to the data [5].

This block-chain technology is transparent technology [6]. Suppose any hacker try to change the data that time automatically detect there some tampering occurred. Because it is transparent and every blocks are interconnected to each other with help oh hashing and that block is shows different to another block. That means it is very secured technology. Any user use this technology for security and privacy purpose in transaction [7]. Block-chain technology contain also use the OTP for security. We know that OTP is most secured password for verified the user. This OTP also increase the complexity of security and privacy. This block-chain connected to the mobile. Mostly the block-chain contain distributed block-chain are used [8]. In this technology contain used the hashing and cryptography algorithm [9]. Cryptography algorithm in which both types are present it is symmetric and asymmetric algorithm. Where public and private key are used and also encryption and decryption are also used. Cryptography algorithm used there for achieve to more confidentiality and enhanced the security. It is much secured transaction process with help of block-chain technology.

1127

It is trusted technology for transfer the data and digital coin. Where used some databases like confidentiality, authentication, authorization, access control, integrity, availability, nonrepudiation and privacy for provide more security [10].

A. **Types of block-chain:**

There are three types:

- **Public Block-Chain:** The public block-chain it is easy to use. This technology contain there is not restriction for use this technology. Everyone used this technology for transaction.
- **Private Block-chain**: The private block-chain it is very difficult for using. Because there need to follows some rules and regulation.
- **Consortium Block-chain**: The consortium block-chain it is free block-chain. There is not particular person directing this technology. Big fields using this technology.

B. **Requirements of Block-chain:**

- **Privacy or Confidentiality**: It is handle to privacy issues, various symmetric and asymmetric key cryptographic system.
- **Integrity**: Integrity provide some quality and it is undividable. It is provided for more security.
- **Availability**: Availability it is provide some quality of process to help for security against hacker and remove tampering.
- **Authentication**: Block-chain provide the authentication for the user is genuine and true for the used this technology.
- **Authorize the technology:** Block-chain provide authorization to giving permission officially to do work on this technology.
- **Access Control**: Access control is a technique of security for which user view or use this technology.
- **Identity Verification**: Block-chain provides one time password, scalability, and mobility that creating new identity verification operation in distributed and trust less weather.
- **Nonrepudiation**: The nonrepudiation provide the some validity of this transaction technology process.

II. PROBLEM DEFINITION

In this section modified block-chain technology with transaction for the purpose to provide more security. This technology provide the solution security and privacy issues of block-chain network with respect to the multiple interconnected devices. In previous project contain security issues were not discussed in block-chain IOT networks. In accordance previous block-chain [1] some importance issue have been discussed in this project as:

A. **Scalable Data Planning**: This is most important issue of block-chain is scalable data planning. Because that rapid growth in their database and enough space are available in this block-chain technology.

B. **Complexity**: Block-chain provide minor to solve some verification issue and authenticate the node of block-chain technology.

C. **Network Speed**: In transaction process not working on time that's reason network speed is more important.

D. **Interoperability**: The block-chain technology contain used the distributed ledger for decentralized the process occurring between users.

E. **Privacy**: block-chain contains multiple people used this technology and their information have to safe it must important.

F. **Standards**: Every technology has their own standard to present their importance in this world.

G. **Regulations and Governance**: In block-chain technology contain some rules and regulation is must important to prevent tampering and secured the data.

III. PROPOSED SYSTEM

In this section, we proposed the project work with some objectives. This is layered framework. In this framework the transmission layer used in again two times. In this framework Fig.4 contain used the perception layer, transmission layer, storage layer and application layer. This framework used for implementing the project work step by step and secured. In this block-chain technology the system are connected to the mobile for provide one time password for more security. In Fig.1 this block-chain technology contain the multiple blocks are interconnected to each other. This block contain the each block of a data, previous hash and current hash are present. Previous hash and current hash are include in hashing algorithm to provide interconnection between two blocks. Hashing algorithm also using for update the block-chain technology and maintain the block-chain technology. In which also using the cryptography algorithm to achieve confidentiality. In this cryptography algorithm contain used the symmetric cryptography algorithm and asymmetric cryptography algorithm for encrypt the data and decrypt the data. In which the perception layer contain the collected the data. Transmission layer contain transmit the data from one user to another user. Storage layer contain the storing data in block memory. Application layer contain the retrieve the data and visualize the data. This is most important layer of block-chain used in transaction. It is secured framework in transaction process. The block chain technology continuously processing with help miners. There need of some computing power. This computing power is centralized miner and they are connected to the multiple nodes. These multiple node means multiple data are present there multiple data means multiple updates are present there. This computing power are used to solve some verifications terms. This computing power also used to reduce some waste of storage and data and protect the technology from the malicious attacks.

A. Objective:

1) **Distributed**: Block-chain contain distributed ledger is most secured for transaction. Because there need not any third trusted party.

2) **Transparency**: In block-chain technology without occurring any tampering the process completed successfully that need some transparency in transaction.

3) **Secured**: In block-chain technology contain using cryptography algorithm for encrypted the data and decrypted the data for security purpose.

4) **Collective Verification**: In BC model verified the user using with OTP.

5) **Privacy**: Block-chain provide the private block-chain technology type for privacy and authorization are used also for privacy.
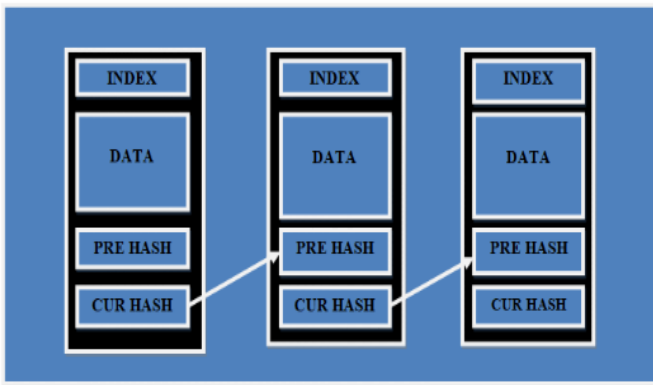
B. Architecture:

Fig. 1. Architecture of Block-Chain Process

A. **Adding Block to The Chain**: The adding new block is the communicated to all the participating nodes to be subsequently appended to the existing chain of blocks with help of hash in the block chain digital ledger.

B. **Creating New Block**: Transaction once approved as valid along with the hash interconnected of the succeeding block are then fed into a new block.

C. **Validation and Verification**:
- This block-chain technology connected to the mobile for providing OTP with more security.
- The transaction now has valid to get approval as being indeed by the block chain system.
- For such a validation and verification process, the participants must apply a specific algorithm and OTP.
- The relevant block chain system defines what is received as valid or authenticate which may vary from one system to another.

D. **Triggering Transaction**: a) Bob is going to transfer some money to Alice.
b) Once the monitory transaction is initiated and hence trigger by Bob, it is represented as transaction

and broadcast to all the involved parties in the network. And giving OTP to logging person and successfully completed the transaction.

C. Principle of Block Chain Addressing:

There are two principle of block chain addressing are follows:

A. **Open Ledger**: The open ledger it is a centralize process ledger.it is exchange the transaction.
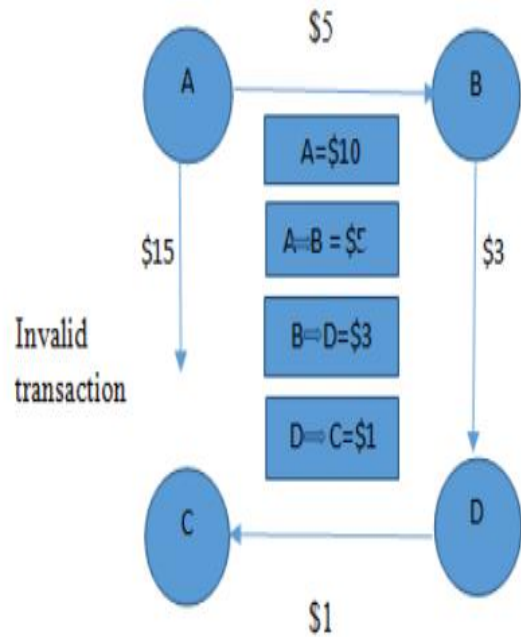

Fig. 2. Open Ledger

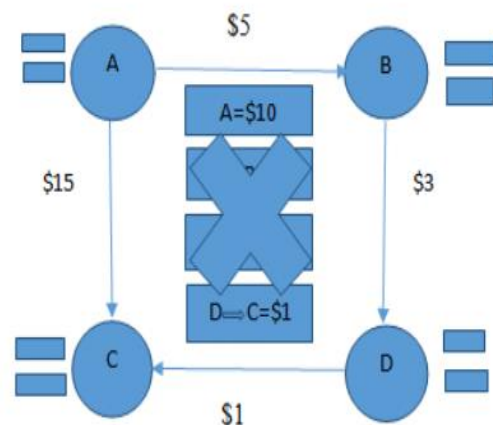B. **Distributed Ledger**: The distributed ledger it is a not centralize process ledger.

Fig. 3. Distributed Ledger
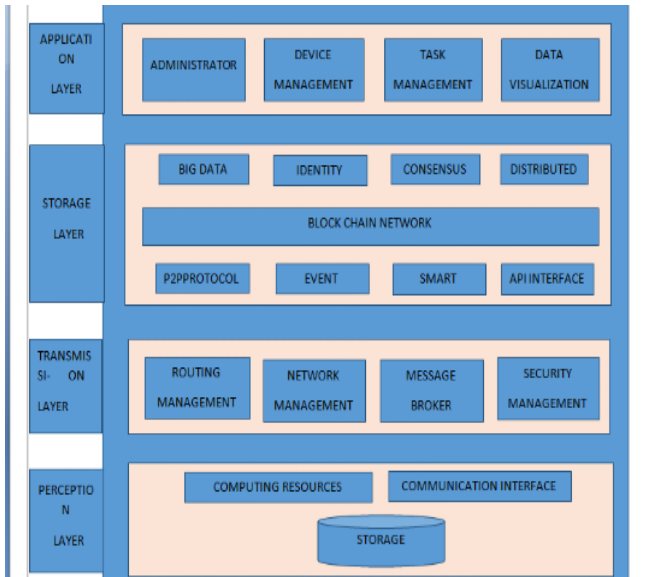
D. Framework:

Fig. 4. Framework Of Block-Chain

A. **Perception BC Layer**:

Block-chain technology of a first layer is perception layer. This layer work is collected the data. In this layer of two main parts. It is encrypted the data and decrypted the data using with cryptography algorithm. Second is hashing the data using with previous hash and current hash.

B. **Transmission BC Layer**:

The second layer of block-chain is transmission layer. Block-chain technology using this layer for the transmitted the data. In which multiple protocol used for transmit the data. Transmission layer of all data are secured in way. It is encrypted data using with some key. Transmission layer contain the occurring communication between users.

C. **Storage BC Layer**:

The third layer of block-chain technology framework is storage layer. This storage layer contain the storing the data in a blocks. In blocks contain some memory are present to soring the data. In which storage layer contain some security is also provided.

D. **Application BC Layer**:

The application layer it is last layer of block-chain technology framework. This framework layer contain the all data are understanding and solved. It is also secured layer of block-chain technology. Where you can asking any questions and getting solution of this question.

IV. METHODOLOGY

A. Cryptographic Algorithm: **Step 1-**

It is used in Fig.4 perception layer of framework. The cryptographic algorithm it is most important algorithm in block-chain technology. Here used for encrypted the users private data for secure transaction e.g. protecting transactional data for not read any third unauthorized party. This cryptographic algorithm used to achieve confidentiality. It is used for security purpose. In which cryptographic algorithm contain encrypt and decrypt the data. In which algorithm contain using the some special key. There is two types of cryptographic algorithm it is symmetric cryptographic algorithm and asymmetric cryptographic algorithm. There public and private of key using in cryptographic algorithm. Where symmetric cryptographic algorithm contain the encrypt the data and send to the receiver using with key then receiver decrypt the data using with same key that is called symmetric cryptographic algorithm. In asymmetric cryptographic algorithm contain the send the data using key with encryption and receiver decrypt the data using with different key that is called asymmetric cryptographic algorithm.

B. Message Time-Stamping: Step 2-

The block-chain technology contain the modification in transactions have to be both signed and time stamped. It is used in Fig.4 transmission layer of framework. Where you can modified the process of block-chain technology. It is time saving of algorithm. All process occurring in times in manner. Where different type of time stamped algorithm are used.

C. Block-chain Updating/Maintenance and Protocol Stack: Step 3-

This technology contain huge number of block-chain devices complete the block and after completion create new block. It is used for updating system. It is used in Fig.4 storage layer of framework. This type of block-chain system contain the system is automatically updating. In which block-chain contain the previous hash and current hash used for the interconnected the block and update the block. This hashing algorithm contain create new block and chain is formed ahead and system automatically maintain. This type devices update their blocks and maintain the blocks.

V. RESULT AND DISCUSSION

1) The result on the block-chain based authentication technique in which using the cryptographic algorithm, hashing algorithm, time stamping, block-chain updating& maintenance and OTP that giving more security. It is easy to utilize the system.
2) It is future scope in smart company, smart school, and smart cities. Also there two principle are available. In block-chain contain the data are automatically update and maintain. There multiple blocks are interconnected to each other. It is a big chain of a data. In which previous hashing and current hashing used for the interconnected to the blocks.
3) Where you can easily transfer the data, money and assets. Here easily you can maintain the privacy. It is transparent and more secured. In transaction process block-chain is most important technology connected with mobile for providing OTP with more security. We know that OTP is more secured. There need not any third trusted party and time saving of this block chain technology.

1130

4) Comparative result with existing system is:

| Block-chain technology	Storage capacity	Cost	Duration capacity
1) Existing system	Less	High	Time consuming
2) Proposed system	High	Less	Time saving

5) Block-chain technology result in modules is:

1) Home page:

This is a homepage. It is main page of a block-chain. Where some information about what is a block-chain. There is some modules are present like that Registration, Login, contact and about us etc.
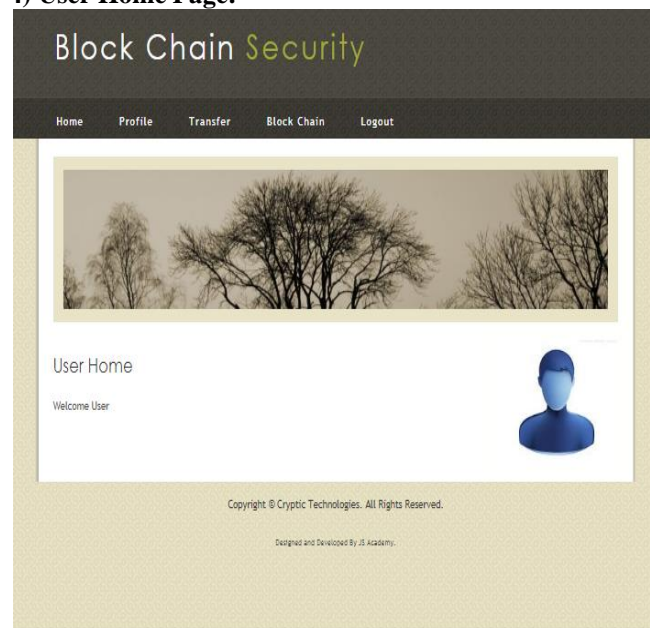
2) Registration page:
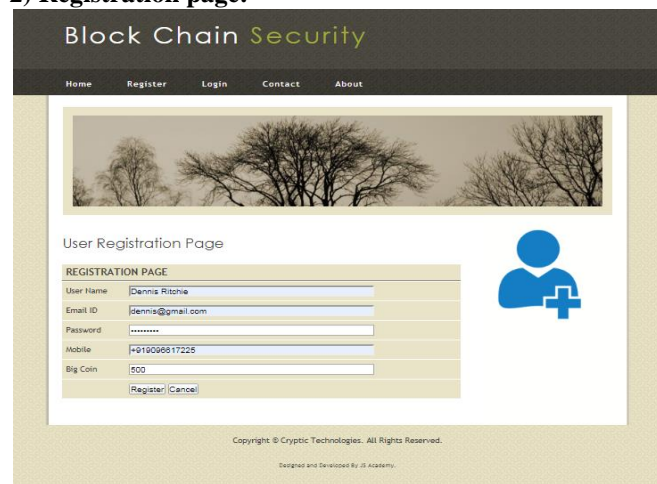
This is a Registration page. Where user can fill the details and register the block-chain technology account. In details contain some name, mobile number, email id, password, and also asking about OTP.

3) Login Page:
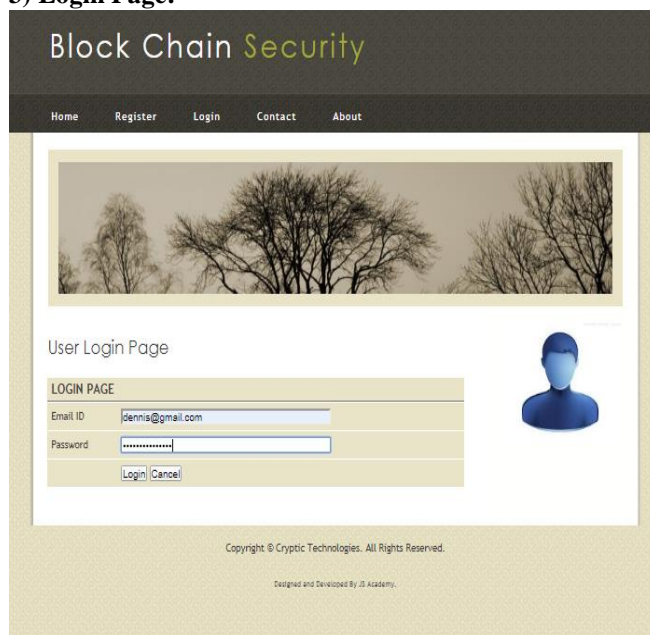
This is a Login page. After successfully registration user will login on this page.

4) User Home Page:

This is a user home page. After successfully login user will come on this page. The home page contain where user can see their profile, transfer the money and also logout their account. In a transfer module contain the user transmit the money using with more security like block-chain security with OTP. In which the system is connected to the mobile for the purpose for OTP.

5) Profile Page:
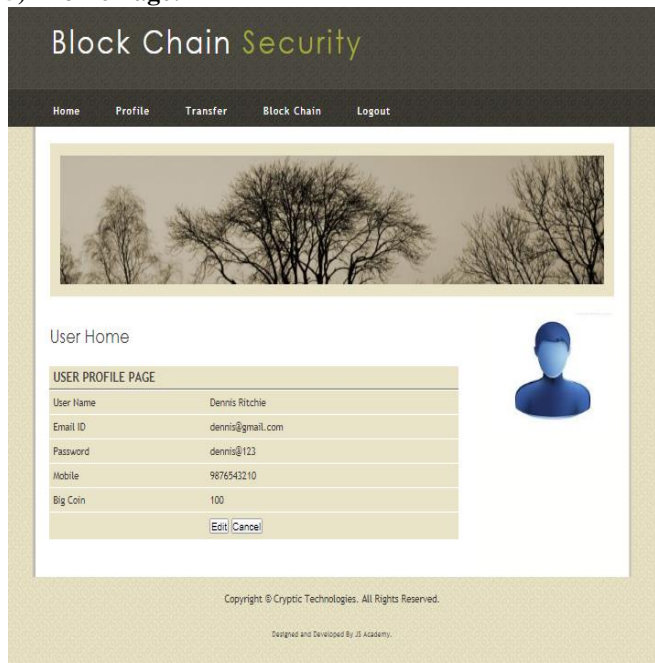
This is profile page. Where users all details are present there. Like Name, Email id, Mobile number and money information. Profile page contain user also edit the profile.

6) Contact Page:
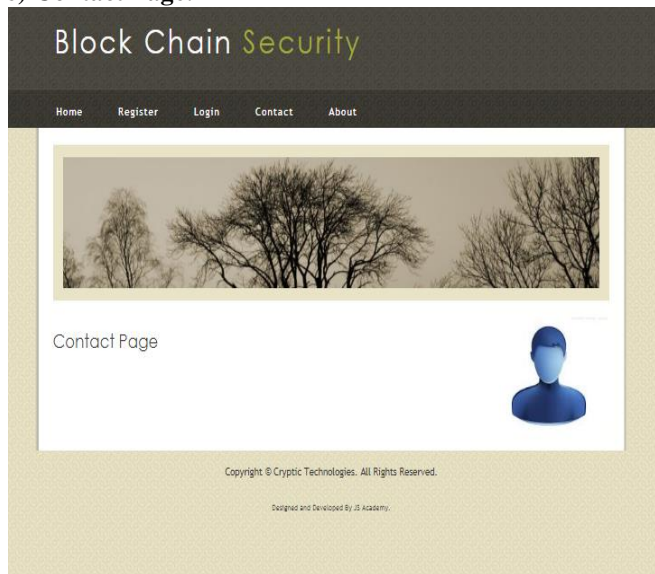
This is a contact page. Where users contacts are present.

6) Result table according to objectives is:

Project Objective	Results
1) Distributed	Yes. Because BC using Decentralized block-chain.
2) Transparency	Yes. Because BC using Hashing algorithm.
3) Secured	Yes. Because BC using Authentication.
4) Collective Verification	Yes. Because using OTP.
5) Privacy	Yes. Because BC using Cryptography algorithm.

Every objective implemented in this project. It is time saving of a transaction. In which cost also decreased.

VI. CONCLUSION

In this paper with help of layered framework fulfilled all the objective is transparency, distributed, secured, collective verification and privacy. In block-chain technology comparative result provided details information about existing and proposed system and drawbacks of existing system. This drawbacks are reason for publish this paper. This block-chain technology based transaction is more secured. Because there multiple blocks are interconnected to each other. This type of interconnection creating the transparency in this transaction. Where using the multiple nodes means multiple data are present there and multiple data means system automatically updated there. This is secured transaction and future scope in companies, education and business purpose. Where using cryptographic algorithm it is used to achieve confidentiality and hashing algorithm used to connect the blocks that is also important for storing data. Using with OTP enhanced their security and privacy. In which used the framework are very systematic. This technology is time saving technology. This technology are used in various field. Generally used every places. It is very secured and flexible of a block-chain technology. It is easy to use. It is verified. Using some rules and regulation we can easily access this technology.

REFERENCES

1. S. Moin, A. Karim, Z. Safdar et "all /Future Generation computersystem"100(2019)325343http://doi.org/10.1016/j.future.2019.053.
2. B. Dorsemaine, "Internet of things a definition & taxonomy, in next generation mobile application service and technology"2015 9th conference on IEEE 2015.
3. M. Devetsikiotis, Christidis, "Block chains and smart contracts for the internet of things" IEEE access 4(2016)2292-2303.
4. Lin T. Liao, "block chain security issues & challenges." 19 (2017)653–659.
5. Ibrar Yaqoob "Internet of things advanced taxonomy requirement and challenges"future general computer syst 92 (2019)265-275.
6. Y. Xu,"A block-chain based non repudiation network computing service scheme for industrial IOT" IEEE india (2019).
7. M. Conoscenti, Vetro "Block-chain for the IOT" a systematic literature in computer system 2016. 13th international conference.
8. N. M. Kumara,"Block-chain technology for security issue and challenges of IOT"computer sci. 132 (2018)1815-1823.
9. A. Reyna, "block-chain challenges & opportunities" future generation comp. syst (2018).
10 K. Salah, IOT security "block-chain solution and challenges" future comp syst 82 (2018)395-411.

AUTHORS PROFILE

Pratiksha P. Gofane, BE Completed in Sipna College of Engineering & Technology Amravati, India. Now Pursuing Master of Engineering Final Year Student of Information Technology in Sipna College of Engineering & Technology Amravati, India. Research work is Implementation of Block-Chain Based Authentication Technique. Email: pratiksha.gofane39@gmail.com.

Dr. Vijay S. Gulhane, Master of Engineering completed in Computer science. And also Phd completed in computer science. Now Professor& Head of Information Technology department at Sipna College of Engineering & Technology Amravati. Teaching Experience is 23 Years. In Journal Publication More than 90 Paper Published. Research work is Implementation of Block-Chain Based Authentication Technique.
Email:vijaygulhane27@gmail.com

Prof. Harshal N. Datir, Master of Engineering Completed in Information Technology and Phd Pursuing in Data Analytics. Now Assistance professor of Information Technology at Sipna College of Engineering & Technology. Teaching Experience is 15 Years. Research work is Implementation of Block-Chain Based Authentication Technique.
Email: harshaldatir809@gmail.com