BLOCKCHAIN BASED AUTHENTICATION SYSTEM

Latha.R[1], Abinaya.S[2], Keerthana.R[3]

[1]Assistan Professor, Department of Information Technology, Veltech High-Tech Dr Rangarajan Dr Sakunthala Engineering College, Avadi

[2,3]Student, Department of information Technology, Veltech, HighTech Dr Rangarajan Dr Sakunthala engineering College, Avadi

---***---

Abstract: *Data security plays a major role in the internet world. Block chain is a distributed and decentralized technology where data is divided and sent in the form of blocks. Layers are replaced with blocks. Which prevents the sent data form hackers. Certificate based security like SSH is used currently. In our work SSH is replaced with blockchain. we have implemented block chain technology to create a login form for a webpage which has integrity check. The process includes division of data into blocks where each block is connected with the other. The last hash value of the current block is the starting hash value of the next block. Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system. A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. Block chain is decentralized and distributed technology. Block chain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system. Any transaction or activity done through block chain technology cannot be hacked. Since block chain does integrity check. When integrity check fails it denies the process. Block chain achieves Authentication, Authorization, Accounting (AAA). Every block is connected with the other the hash value. The last value of the first block and the starting value of the second block should match. The very first block of the chain is known as genesis block or 0th block. The genesis block is the very first block in any blockchain based protocol. It is the basis on which additional block are added to form a chain of blocks. This is block is referred as 0 every block in a block chain stores a reference of the previous security plays a major role in the internet world. Block chain is a distributed and decentralized technology where data is divided and sent in the form of blocks . Layers are replaced with blocks. Which prevents the sent data form hackers. Certificate based security like block. In the case of genesis there is no previous block for reference. This means that there is no data processed before the genesis block.*

Keywords: SSH, AAA, Blockchain

I.INTRODUCTION

Data SSH is used currently. In our work SSH is replaced with blockchain. we have implemented block chain technology to create a login form for a webpage which has integrity check. The process includes division of data into blocks where each block is connected with the other. The last hash value of the current block is the starting hash value of the next block. Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system. A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. Block chain is decentralized and distributed technology. Block chain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system. Any transaction or activity done through block chain technology cannot be hacked. Since block chain does integrity check. When integrity check fails it denies the process. Block chain achieves Authentication, Authorization, Accounting (AAA). Authentication refers to a unique username and password. Authorization is refered as the process of adding or dening a individual user to access the network. Acconting refers to the process of monitoring user activity on a network. Every block is connected with the other with the hash value The last value of the first block and the starting value of the second block should match .The very first block of the chain is known as genesis block or 0th block. The genesis block is the very first block in any block chain based protocol. It is the basis on which additional block are added to form a chain of blocks. This is block is referred as 0 every block in a block chain stores a reference of the previous block. In the case of genesis there is no previous block for reference. This means that there is no data processed before the genesis block.

1.1 INTRODUCTION TO BLOCK CHAIN

Block chain is decentralized and distributed technology. Block chain is a system of recording information in a way

---

that makes it difficult or impossible to change, hack, or cheat the system. Any transaction or activity done through block chain technology cannot be hacked. Since block chain does integrity check. When integrity check fails it denies the process. Block chain achieves Authentication, Authorization, Accounting (AAA).

II.RELATED WORKS

A. A BLOCKCHAIN BASED ACCESS AUTHENTICATION SCHEME OF ENERGY INTERNET

ABSTRACT:

In this paper, proposed system uses blockchain technology as a distributed authentication scheme for energy internet. Energy Internet refers to combination of advanced power and electronics technology. A secure and efficient access is given for energy internet which is based on decentralised technology.

AUTHORS & YEAR: Ammar Ayman, Mohammad moussa madine, Hamad Alzaabi Ibrar Yaqoob, Khaled Salah, Raja Jayaraman(2020)

B.DESIGNING AUTHENTICATION AND AUTHORIZATION SYSTEM USING BLOCKCHAIN TECHNOLOGY

ABSTRACT: In this paper, blockchain is used as a database for storing credentials. Based on the information received the users and services can perform authentication and authorization.

AUTHORS & YEAR: Yuki Ezawa, Makoto Takita,Yoshiaki shiraishi, Shohei Kakei, Masanori Hirotomo, Misami Mohri, Masakatu Morii(2019)

C. DECENTRALIZED ACCESS CONTROL INFRASTRUCTURE USING BLOCKCHAIN FOR BIGDATA

ABSTRACT:

The security and privacy issues in big data are enlarged. So in this paper, By using blockchain technology a proposed system created an decentralized access control infrastructure.

AUTHORS & YEAR: Oussama mounnan, Anas Abou El kalam, Lamina El Haourani(2019)

D. BLOCKCHAIN FOR DECENTRALIZED DATA ANALYSIS

ABSTRACT:An early stage of work in decentralized data analysis is described in this paper. It describes issues faced during setting up the decentralized environment by using blockchain to support data for analysis.

AUTHORS & YEAR: Monica Nugent, Ruth G Lennon(2019)

E. DAuth - A DECENTRALIZED WEB AUTHENTICATION SYSTEM USING ETHEREUM BASED BLOCKCHAIN

ABSTRACT:This paper proposed a system that uses an OAuth 2.0 based authentication. In this 3rd party authentication provider has the control of user data, they can decide whether the data should be modified or to be leaked. An alternative way of authentication service has been proposed based on blockchain and its usecases.

AUTHORS & YEAR: Shibasis Patel, Anisha sahoo, Bhabendu Kumar Mohanta, Sowmyashree S Panda, Debasish Jena(2019)

F. AN PRIVACY–PRESERVING CROSS ORGANIZATIONAL AUTHENTICATION/ AUTHORIZATION/ACCOUNTING SYSTEM USING BLOCKCHAIN TECHNOLOGY

ABSTRACT:By using a virtual coin exe_coin proposed system provides authentication, authorization, accounting functions to achieve accouting function. To adapt the transparency feature of blockchain, one-way hash chain is used.

AUTHORS & YEAR: Peggy joy Lu, Lo Yao Yeh, Jing-Long Huang(2018)

G. AN AUTHENTICATION SCHEME USING IDENTITY BASED ENCRYPTION AND BLOCKCHAIN

ABSTRACT:

In this paper, based on identity based encryption a new authentication scheme is proposed and blockchain is used. Key management issue can be simplied by identity-based encryption, still it suffers from some drawbacks.

AUTHORS & YEAR: Beini Zhou, Hui Li, Li Xu(2018)

H. BLOCKCHAIN BASED MUTUAL AUTHENTICATION SECURITY PROTOCOL FOR DISTRIBUTED RFID SYSTEM

ABSTRACT:

This paper uses a radio frequency identification technology. In this system there is no need for third parties to provide security.

AUTHORS & YEAR: Siye Wang, Shaoyi Zhu, Yanfang Zhang(2018)

III.PROPOSED SYSTEM

The proposed system in this project is to create a login form for a webpage using blockchain technology. To improve the security features we are using blockchain technology where as in the existing system secure shell protocol is used in which the data is sent in the form of layers which can be hacked easily whereas in blockchain, data is sent in the form of block. So, hacking a block is not that easy. We propose a blockchain based authentication system, in this new system we include integrity check.

3.1 SYSTEM ARCHITECTURE

Start the process. The user have number of attempts. In login, the user should give their username, password and phone number. After entering the phone number otp is generated. Then it is divided into number of blocks. Each block contains two hash values(previous hash value, before hash value). In integrity check, by checking the last hash value of the first block and starting value of the second block we can identify whether the data is modified or not. If it is same then the access is valid otherwise it is invalid. If the user put invalid password and username then the process won't take place.
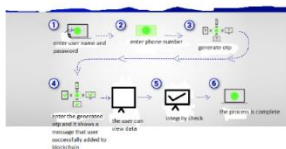
3.2 PROGRAMMING FILES

We have implemented 6 python programming files into a single program file and they are

1. Block.py
2. Genesis.py
3. Checkchain.py
4. Getblock.py
5. Newblock.py
6. Blockchain.py

1. BLOCK.PY:
Block.py is a python module which here will store the property of each block. Hashlib is imported to store the hashvalue. Index, timestamp, data, previous hash are the properties of a block.

2. GENESIS.PY:
Genesis block is nothing but the very first block of the chain   it is also known as zeroth block. Genesisblock.py is a python module that is designed for the creation of the very first block.

3. GETBLOCK.PY:
Getblock is used to get new block.

4. NEWBLOCK.PY:

It contains the properties of new block. The properties of new block are previous hash, timestamp, index, data.

5. BLOCKCHAIN.PY:
This is our main program where all the previously created modules are implemented. We are importing datetime, flask, request, render template, response. Flask is used for creating a user interface. Render template helps to run the code on local host.

IV.SYSTEM MODULES

The various modules in this project are 1.Homepage

2.Login page

3.Display data

4.Integrity check

1. HOME PAGE:
Home page is the initial page which is displayed. where the user will enter their name.

2. LOGIN PAGE:
Login page is the second page in which the user have to enter the username and password. Here the date will be generated automatically since we have imported datetime library. Then the user will be displayed with a page saying that the credentials are added to the blockchain.

3. DISPLAY DATA:
In this page the user can view their data. They have to enter name the they will be able to view their username password and time.

4. INTEGRITY CHECK:

In this page the system will do integrity check process. Integrity check is the process of checking whether the data in the chain is modified or not by checking the length of the data if length remains same then no modifications are occurred.

V. RESULT

In existing system, communication is based on seven layers and no integrity check in current technology. To address these problems, we propose a blockchain based authentication system. In this new system we include integrity check and also we use secure hash algorithm 512 to hash the block.
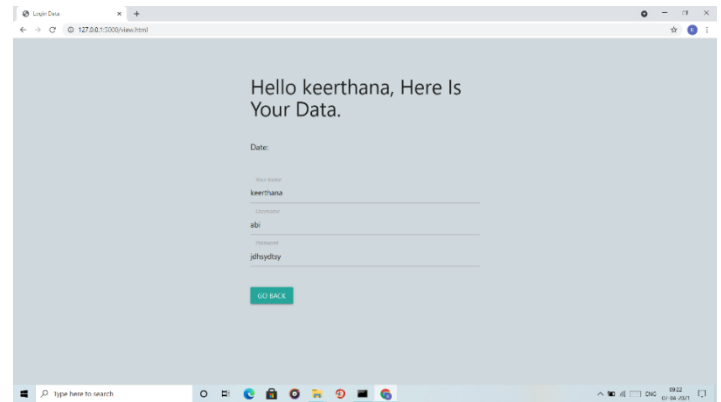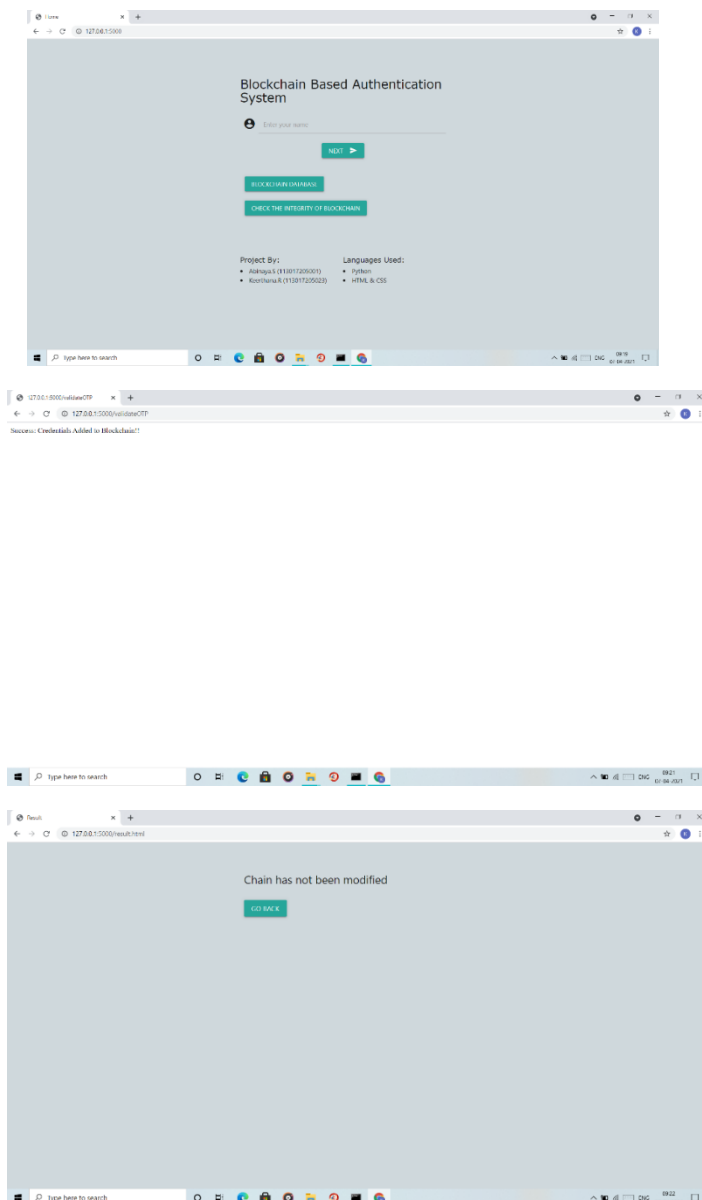
VI.CONCLUSION

By implementing blockchain technology, data can be stored in more secure manner. Blockchain has the ability to check if the connection is tampered. The data will be more secure and unhackable than the existing system. Data can be retrived only by the authorized user.

REFERENCES

[1] Ammar Ayman, Mohammad moussa madine, Hamad Alzaabi Ibrar Yaqoob, Khaled Salah, Raja Jayaraman, "Block chain based multi party authorization for accessing IPFS encrypted data", 2020.

[2] Yuki Ezawa, Makoto Takita, Yoshiaki shiraishi, Shohei Kakei, Masanori Hirotomo, Misami Mohri, Masakatu Morii, "Designing authentication and authorization system using block chain technology", 2019.

[3] Oussama mounnan, Anas Abou El kalam, Lamina El Haourani, "Decentralized access control infrastructure using bock chain for big data", 2019.

[4] Monica Nugent, Ruth G Lennon, "Block chain for decentralized data analysis", 2019.

[5] Shibasis Patel, Anisha sahoo, Bhabendu Kumar Mohanta, Sowmyashree S Panda, Debasish Jena, "DAuth - A decentralized Web authentication system using ethereum based blockchain", 2019.

[6] Peggy joy Lu, Lo Yao Yeh, Jing-Long Huang, "An privacy – preserving cross organizational authentication/authorization/accounting system using blockchain technology", 2018.

[7] Beini Zhou, Hui Li, Li Xu, "An authentication scheme using identity based encryption and block chain", 2018.

[8] Siye Wang, Shaoyi Zhu, Yanfang Zhang, "Block chain based mutual authentication security protocol for distributed RFID system", 2018.