Data Security By Using Blockchain With Fog Node

BHILESH BHUDE [1], SURAJ DESHMUKH [2], RUPESH MESHRAM [3] ,ANURAG CHETULE[4],DIPEEKA RADKE[5]

COMPUTER SCIENCE AND ENGINEERING, PRIYADARSHINI BHAGWATI COLLEGE OF ENGINEERING, NAGPUR
COMPUTER SCIENCE AND ENGINEERING, PRIYADARSHINI BHAGWATI COLLEGE OF ENGINEERING, NAGPUR
COMPUTER SCIENCE AND ENGINEERING, PRIYADARSHINI BHAGWATI COLLEGE OF ENGINEERING, NAGPUR
COMPUTER SCIENCE AND ENGINEERING, PRIYADARSHINI BHAGWATI COLLEGE OF ENGINEERING, NAGPUR
COMPUTER SCIENCE AND ENGINEERING, PRIYADARSHINI BHAGWATI COLLEGE OF ENGINEERING, NAGPUR

---***---

Abstract -Nowadays, the production and usage of the Internet of Things devices are increasing very rapidly. IoT devices are resource-constrained devices, incapable of securing and defending themselves, and can be easily hacked and compromised.The primary goal of this project is to propose and analyze the security by using authentication scheme at scale for IoT devices.This project can be used in Data Security, to maintain or store database. In this project we can firstly encrept the data which is given from user that data will store in mysql Database then Decrypted data before decreption it will create tokens or generate key, using that key the data will download from Database. The Data inside the Database will be download data only when the generated key will be same as input key. The application consists of Bitcoin for maintaing the history of transaction, Smart City, Commercial Real Estate, Cyber Law, Data Strorage.

Key Words:IoT, IoT Security, Blockchain,,Authentication.

1.INTRODUCTION

Nowadays, the production and usage of the Internet of Things devices are increasing very rapidly2020. As opposed to endpoint devices, IoT devices are resourceconstrained devices, and are incapable of securing and defending themselves, and can be easily hacked and compromised. Therefore, it is important to adopt proper schemes for authenticationand control access to ensure the overall security for IoT devices, their communications, and their data.the authentication scheme must be reliable, scalable, and secure against known attacks and threats.Moreover, research communities as a distributive technology that plays major role in managing, controlling, and most importantly securing IoT devices.Blockchain can be a key enabling technology for providing viable securitysolutions to todays challenging IoT security problems.To overcome the drawbacks of the centralized based authentication, a decentralized authentication scheme using fog nodes and blockchain technology is proposed in this paper. This scheme or technology will provide security without need of Trusted Third Party. The Data which is store in the Database will be downloaded after checking the Tokens which will issued by the smart contracts with no intermediary or trusted third party.

2. LITERATURE SURVEY

Dynamic search-able symmetric encryption

S. Kamara, C. Papamanthou, and T. Roeder

Searchable symmetric encryption (SSE) allows a client to encrypt data in such a way that it can later generate search tokens to send as queries to a storage serve. We propose the first SSE scheme to satisfy all the properties like sub-linear search time and so-on. Extends the inverted index approach in several non-trivial ways and introduces new techniques for the design of SSE. We implement our scheme and conduct a performance evaluation, showing that our approach is highly efficient and ready for deployment.

Efficient no-dictionary verifiable SSE

W. Ogata and K. Kurosawa

A generic method to transform any SSE scheme (that is only secure against passive adversaries) to a no-dictionary verifiable SSE scheme. A client encrypts a set of files and an index table by a symmetric encryption scheme, and thenstores them on an untrusted server. In the search phase, he can efficiently retrieve the matching files for a searchkeyword w keeping the keyword and the files serve.

3. METHODOLOGY

To overcome the security problems that are occurred in the existing system and effectively store the data over the cloud we introduce this system.
Every transaction in the ledger is digital signed and validated by tens of thousands of mining nodes in the network.
Transactions are stored and organized by time stamps in groups called blocks. These blocks are linked (or chained) together to form a chain of blocks, or a block chain. The block chain uses AES scheme to provide strong cryptographic proof for data authentication and integrity.

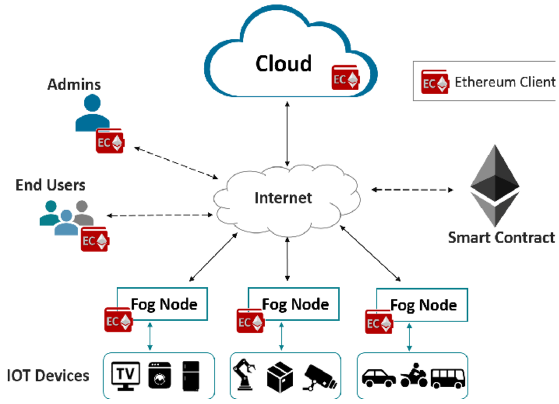


Fig.Proposed system architecture with ethereum enabledfog nodes.

The following summarizes the key role of the different system participants:

1) **Admins:** Admins are responsible for managing the user access control and permissions for IoT devices. We assume there can be multiple admins in an organization with management control. The admin in the system is the owner or the creator of the smart contract. A single Contract cannot handle whole system he appoint or add other user as an admin.

2) **End Users:** End users are the customers who request access permission from the smart contract to access a certain IoT devices. Once the users are granted access permission via the smart contract, they contact the designated fog node responsible for managing the targeted IoT device for authentication and access.

3) **Smart Contract:** A single smart contract is used in our proposed solution for the whole system. It is small computer program. It will not involvement of third trusted party. All registration, authentication, access control functionalities are governed in a decentralized manner through the smart contract.

4) **Fog Nodes**: The fog nodes are also used in managing access to IoT devices. Each fog node is handling a group of IoT devices. The fog node relieves the IoT devices from the burden of the storage, memory, and computation load involvedin the authentication process and interfacing with the Ethereum network.

5) **IoT Devices:**Each IoT device in the system is mapped to one fog node. In this paper, we show only our solution for user authentication and access, but it is worth noting that access and authentication of severs to IoT devices can be carried out in similar manner as done for the end users.

4. DESIGN AND IMPLEMENTATION

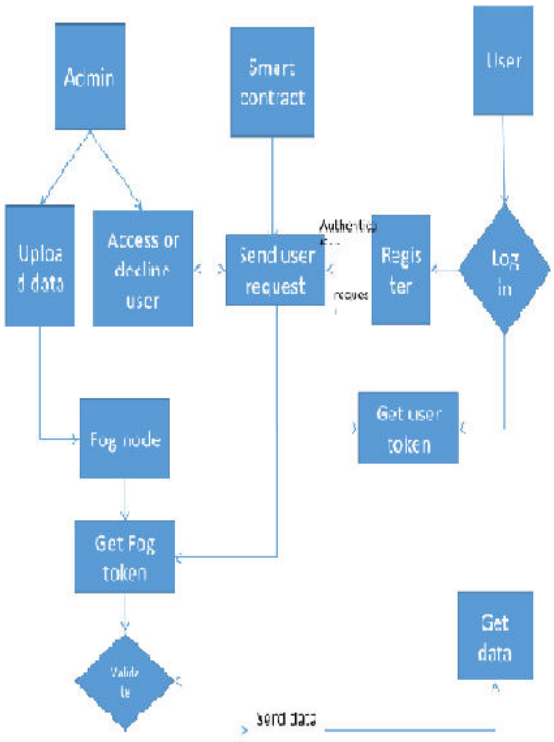


Fig. Flow diagram of Data Security using Blockchain with Fog Node

1. USER AUTHENTICATION

User authentication is a process that allows a device to verify the identity who connects to a network resource. The identity of user is check by identifying username and password.

In registration process user has to input their details like user name, email address and the password they want to access.

The authentication through this process is very efficient.When a user wants to log in, then the user first types username and password.

2. FILE UPLOAD

There is a presence of huge number of computers, which is uploading the file from one computer to another from that computers.

From the user point of view the file is send from one computer to another computer which will receive it.

3. ADMIN ACESS

Admins are entities responsible for managing the access control and permissions for uploaded file. . We assume there can be multiple admins in an organization with management control. The admin in the system is the owner or the creator of the smart contract. The already system Admin can make other users to be the admin.

4. SMART CONTRACT

It is the simple computer Program. A single smart contract is used in our proposed solution for the whole system. Which is used to create tokens and avoid trusted third party services this process at the backend.

All registration, authentication, access control functionalities are governed in a decentralized manner through the smart contract.

5. ENCRYPT FILE AND BLOCK CREATION

The data is encrypted for secure purpose. So that the unauthorized person cannot be able to access the data that are presented in the cloud..

A blockchain, originally block is a growing list of records called blocks.

6. KEY GENERATION

In this module will generate a key using AES (Advanced Encryption Standard) algorithm.The key is used for authentication purpose.

The generated key will send to the user to decrypt their data.

It includes key servers, user procedures, and other relevant protocols.

7. FILE DOWNLOAD

The encrypted documents are keep them safe in the cloud for searching the data user must get the key.

Getting the key is the only way to get the decrypted file. If the key will wrong then will not download encrypt file.

Encryption and decryption of the file uses the AES algorithm and the key is also generated by the AES (Advanced Encryption Standard) technique.

In this module user can search for their uploaded file which is stored in the cloud.

They will get the decrypted file after the key generated by the AES in the server.

In this module, Authentication of the key is being processed, after completion of the successful authentication the file is retrieved from the server in a decrypted form.

5.RESULT

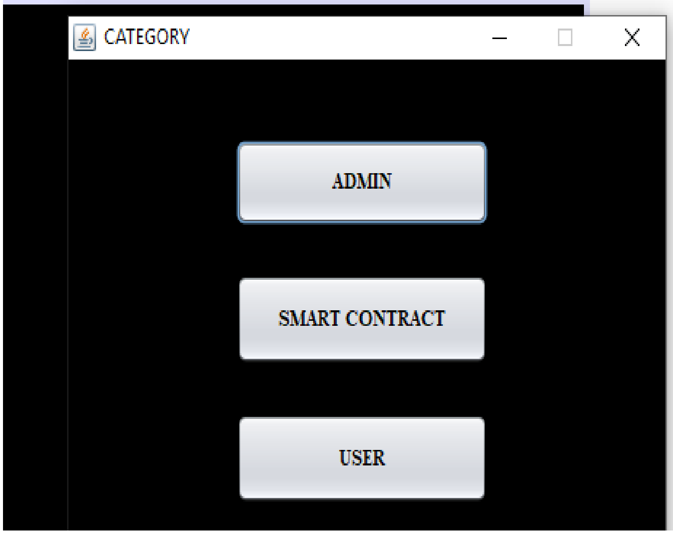


Fig. Home Page

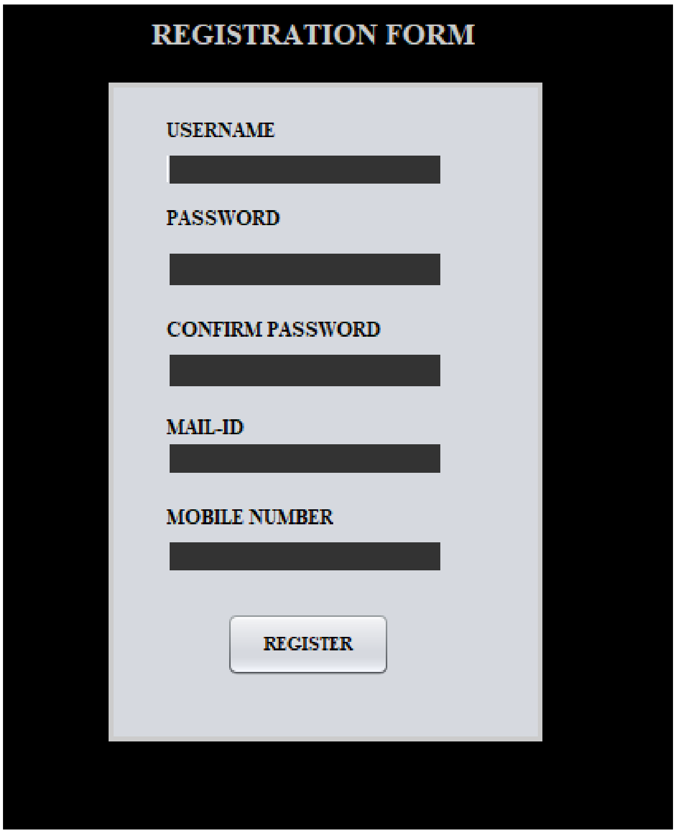


Fig. Registration Form

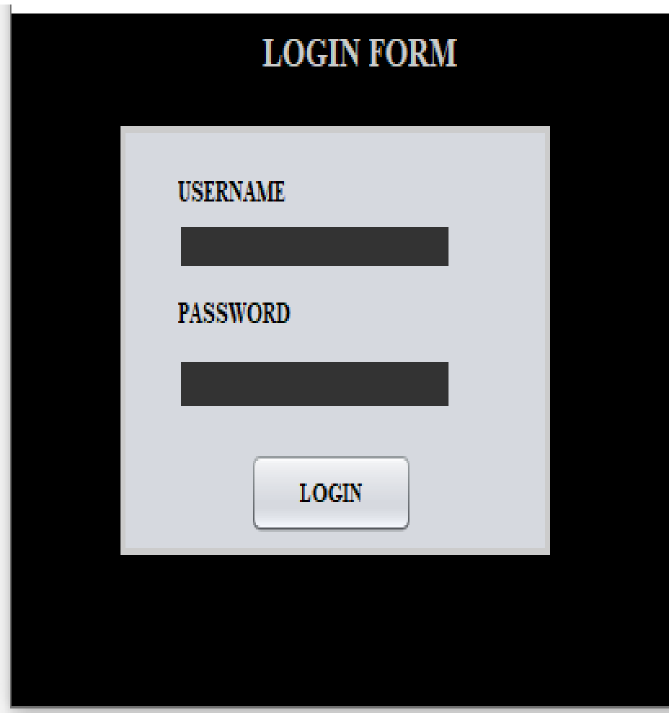
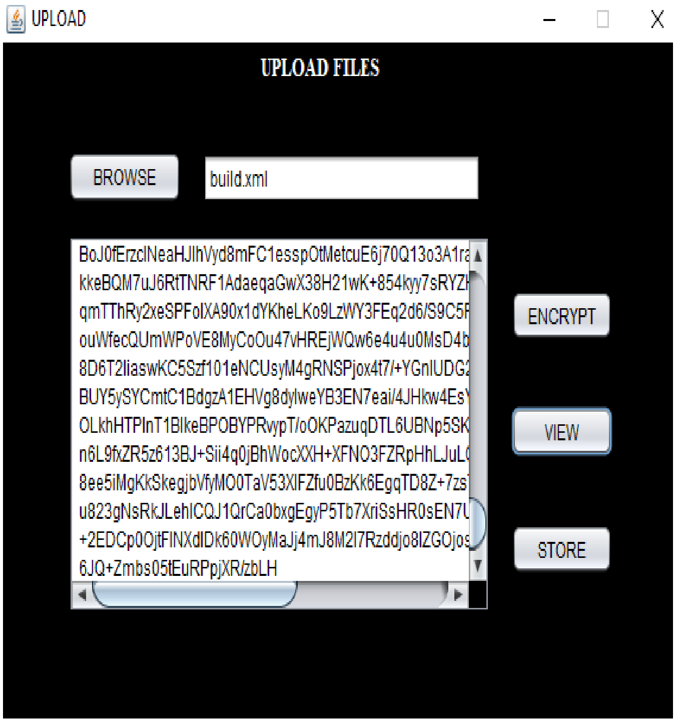
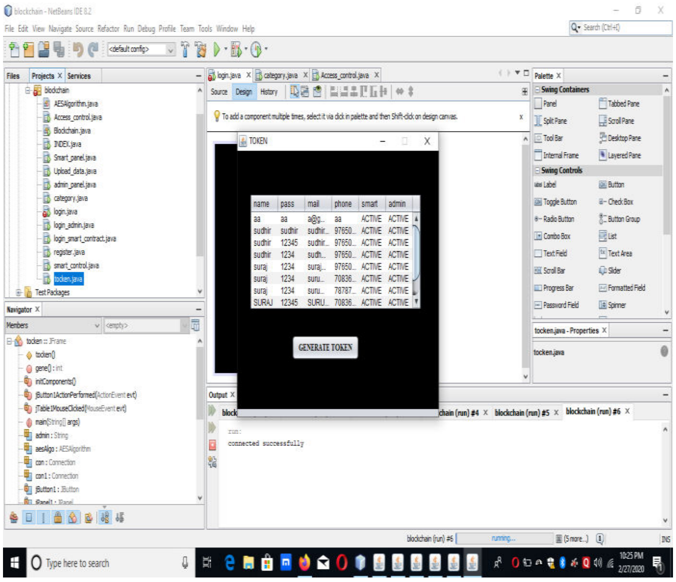


Fig. Login Form



```
BoJ0fErzclNeaHJlhVyd8mFC1esspOtMetcuE6j70Q13o3A1ra
kkeBQM7uJ6RtTNRF1AdaeqaGwX38H21wK+854kyy7sRYZH
qmTThRy2xeSPFoIXA90x1dYKheLKo9LzWY3FEq2d6/S9C5F
ouWfecQUmWPoVE8MyCoOu47vHREjWQw6e4u4u0MsD4b
8D6T2liaswKC5Szf101eNCUsyM4gRNSPjox4t7/+YGnlUDG2
BUY5ySYCmtC1BdgzA1EHVg8dylweYB3EN7eai/4JHkw4EsY
OLkhHTPInT1BIkeBPOBYPRvypT/oOKPazuqDTL6UBNp5SK
n6L9fxZR5z613BJ+Sii4q0jBhWocXXH+XFNO3FZRpHhLJuL
8ee5iMgKkSkegjbVfyMO0TaV53XlFZfu0BzKk6EgqTD8Z+7zs
u823gNsRkJLehlCQJ1QrCa0bxgEgyP5Tb7XriSsHR0sEN7U
+2EDCp0OjtFINXdIDk60WOyMaJj4mJ8M2I7Rzddjo8IZGOjos
6JQ+Zmbs05tEuRPpjXR/zbLH
```

Fig. File Upload For Encryption



To add a component multiple times, select it via click in palette and then Shift-click on design canvas.

name	pass	mail	phone	smart	admin
aa	aa	a@g...	aa	ACTIVE	ACTIVE
sudhir	sudhir	sudhir...	97650...	ACTIVE	ACTIVE
sudhir	12345	sudhir...	97650...	ACTIVE	ACTIVE
sudhir	1234	sudh...	97650...	ACTIVE	ACTIVE
suraj	1234	suraj...	97650...	ACTIVE	ACTIVE
suraj	1234	suru...	70836...	ACTIVE	ACTIVE
suraj	1234	suru...	78787...	ACTIVE	ACTIVE
SURAJ	12345	SURU...	70836...	ACTIVE	ACTIVE

```
run:
connected successfully
```

Fig. Generate Token and Download File

6. CONCLUSION

We have proposed a system design, and implementation of a Block chain-based solution using Ethereum smart contracts for IoT devices authentication at scale, in a decentralized manner with no intermediary third party. We implemented the proposed Ethereum smart contract. Authenticating large scale of IoT devices is featured by involving fog nodes which are used to relieve the IoT devices from the processing burden of carrying out authentication tasks and the connectivity overhead involved with interfacing with the Ethereum Block chain network.

7. REFERENCES

[1] S. Z. Syed Idrus| E. Cherrier| C. Rosenberger| and J.-J. Schwartzmann|"A review on authentication methods|" vol. 7, pp. 95–107, 06 2013.

[2] M. A. Khan and K. Salah, "Iot security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, vol. 82, pp. 395 – 411, 2018. [Online]. Available: http://www.sciencedirect. com/science/article/pii/S0167739X17315765 L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," pp. 254–269, 10 2016.

"Making smart contracts smarter," pp. 254–269, 10 2016.

[3] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the internet of things," CoRR, vol. abs/1802.04410, 2018. [Online]. Available: http://arxiv.org/abs/1802. 04410

[5] S. Cirani, M. Picone, P. Gonizzi, L. Veltri, and G. Ferrari, "Iot-oas: An oauth-based authorization service architecture for secure services in Iot scenarios," IEEE Sensors Journal, vol. 15, no. 2, pp. 1224–1234, Feb 2015.