International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.089|

||Volume 9, Issue 4, April 2020||

Intelligence Bureau Communication Application by Using Blockchain with the combination of centralized servers

Apoorva Nampalliwar [1], Vrushali Choudhary[2], Akshay Mohokar [3], Ankush Chaudhary [4], Nilima Pardakhe[5]

B.E. Student, Department of Computer Science and Engineering, Prof. Ram Meghe Institute of Technology and Research, Badnera, Maharashtra, India[1,2,3,4]

Assistant Professor, Department of Computer Science and Engineering,Prof. Ram Meghe Institute of Technology and Research, Badnera, Maharashtra, India[5]

ABSTRACT: A blockchain is essentially a distributed database of records or public ledger of all transactions or digital events that have been executed and shared among participating parties. Cloud technology is becoming very popular now-a-days. One of the advantages of cloud is centralized server and database. In cloud computing, the data and documents are maintained on one server only. Although there are many advantages of centralized server, there is a possibility that the curious administrator leak or access customer's important documents. Therefore to solve this issue we proposed a secure communication system which will be the combination of centralized data storage as well as distributed data storage. In this system, we proposed a secure group as well as one to one communication for the employees in intelligent Bureau. To increase security of the messages, we will use blockchain technology for message storage. As we can store only messages with limited size in blockchain, we proposed a separate Interplanetary File Server to store big documents.

KEYWORDS: Blockchain, Intelligence Bureau, Communication Application, Cloud Computing.

I. INTRODUCTION

Communication in intelligent Bureau system is very important and hence it should keep secure from third party attackers, administrators and other users. Therefore in this project we proposed hybrid architecture for communication system. Hybrid refers to the combination of centralized server as well as blockchain miners. In this project, the basic data related to employee's profile, groups, cases, group members etc. will be maintained on centralized server and communication messages will be stored in blockchain. Generally, there are live users to handle miners (i.e. Blockchain servers), but in our project we proposed a random technique to choose miner for message transaction processing. In our project, we will store encrypted messages in blockchain and their keys will be maintained on centralized server. As the data is scattered, possibility of data leakage is reduced. Along with communication message we also consider big documents/ attachments. The attachments will be stored separately on **interplanetary server. Interplanetary Server** is a separateserver in which the files will be maintained. Along with Interplanetary Server, we will maintain the backup copy of the same document on any of the blockchain miner server. The address of the document will be stored in blockchain rather than complete file. In this project we are using AES algorithm for document encryption and SHA algorithm for Hash value calculation in blockchain implementation.

II. LITERATURE REVIEW

Blockchain technology keeps a continuous, fixed record list, called blocks, which are linked and secured using cryptographic functions. Each block usually contains transaction data, timestamp and hash which is a pointer to the previous block. It is an open and distributed ledger that can record transactions between two parties effectively, verifiably and permanently. The blockchain was developed as a solution to the Byzantine general's problem. It is secure

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.089|

||Volume 9, Issue 4, April 2020||

by design and is an example of a transparent and fast distributed computing system. There is a potential for using it in identity management, transaction records, documentation of resources, food traceability, voting systems and similar record management activities. Blockchain systems are widely used for the crypto currency today. The identity verification (authentication) is mostly done by a symmetric cryptology.IPFS is a hypermedia distribution protocol created to make the web faster, safer, and more open. It is designed to provide a decentralized alternative to the current HTTP protocol that is censorship resistant and much more efficient. IPFS is a peer-to-peer distributed file system that aims to connect all computing devices with the same file system.

III. OBJECTIVES

- To develop an inter group communication system for Intelligence Bureau .
- To develop an IPFS (InterPlanetary File System) for document storage.
- To implement block chain technology for communication system.

IV. PROPOSED WORK

Step wise working of block diagrams:-

- The admin will create the accounts of new employees.
- With the help of user-id and password the user will login into the application.
- On the groups formed by admin the employees will interact with eachother.
- The message will be encrypted with unique hash value and stores that file into IPFS server.
- Then the message is decrypted by the authenticated user and through which they can communicate with each other.
- In case the data has lost, the backup server can restore the data.

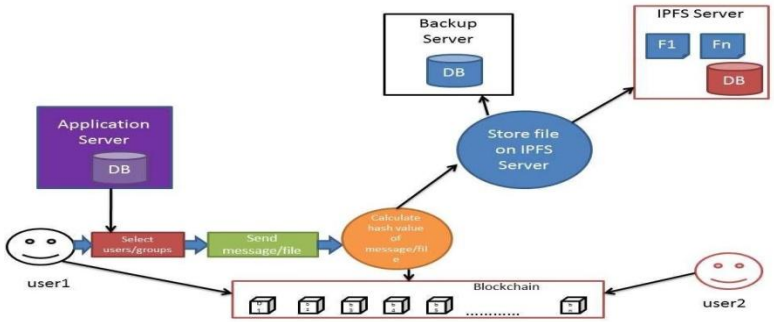


Fig 1: Block diagram of system

Interplanetary File System (IPFS) is a protocol and network designed to create a content- addressable, peer-to-peer method of storing and sharing hypermedia in a distributed file system. Similar to a torrent, IPFS allows users to not only receive but host content.

- IPFS with blockchain ispreferred.
- Blockchain technology is not fit to store large amounts ofdata.
- IPFS is selected to overcome this and the system will be designed to be used as a publicly accessibledatabase.
- On the IPFS each file submitted to the network is given a unique cryptographic hash that allows the IPFS network to automatically delete duplicates and track version history for everyfile.

- Historic versioning prevents information from being easily erased. Since the files are provided by distributed nodes, download speeds arehigher.

These characteristics make the IPFS a perfect place to store data, which can be referenced and time stamped with blockchain technology.

V.MODELLING OF STRUCTURE

4.1 Algorithms:-

In this project we proposed following algorithms to improve transaction security

- SHA algorithm for hashing in block chain
- AES

4.1.1 SHA Algorithm:

SHA-256 is a member of the SHA-2 cryptographic hash functions designed by the NSA. SHA stands for Secure Hash Algorithm. Cryptographic hash functions are mathematical operations run on digital data; by comparing the computed "hash" (the output from execution of the algorithm) to a known and expected hash value, a person can determine the data's integrity. A one-way hash can be generated from any piece of data, but the data cannot be generated from the hash.

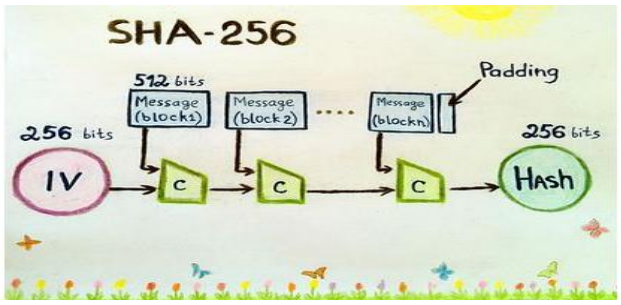


Fig 2: SHA-256 Design

4.1.2 AES Algorithm:

The Advanced Encryption Standard, or AES, is a symmetric block cipher chosen by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data. The National Institute of Standards and Technology (NIST) started development of AES in 1997 when it announced the need for a successor algorithm for the Data Encryption Standard (DES), which was starting to become vulnerable to brute-force attacks.

4.2 Data Flow Diagram:

4.2.1 Account Management:

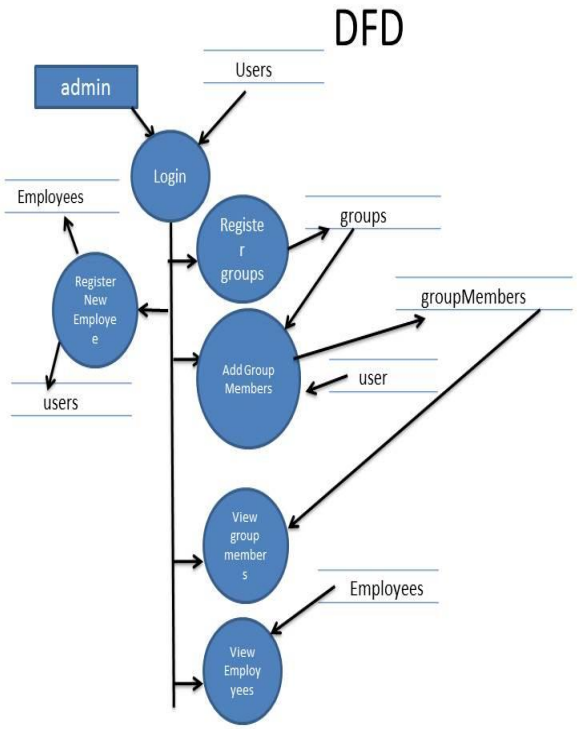


Fig 3: Data Flow Diagram for Account Management

4.2.2 Message Transaction:

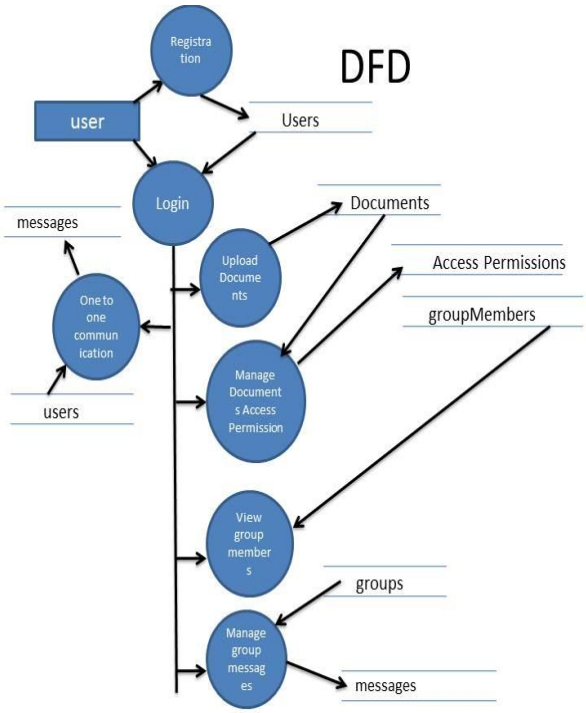
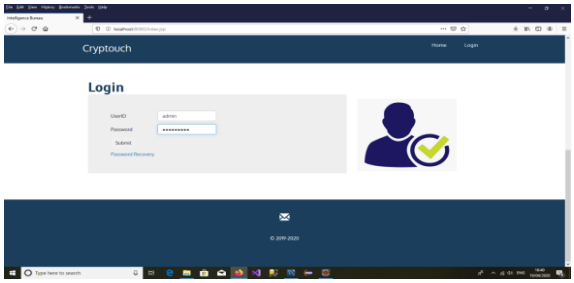


Fig 4: Data Flow Diagram for Message Transaction

VI. RESULTS AND DISCUSSIONS

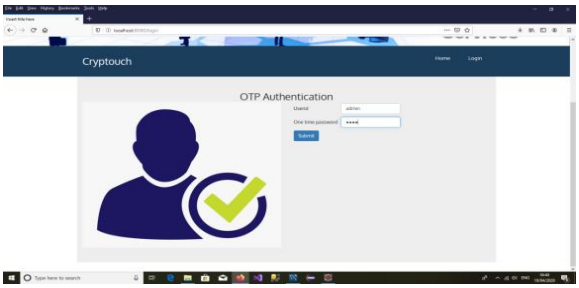
1. Login Page

Admin or User (Employee) can login here by entering associated userid and password.



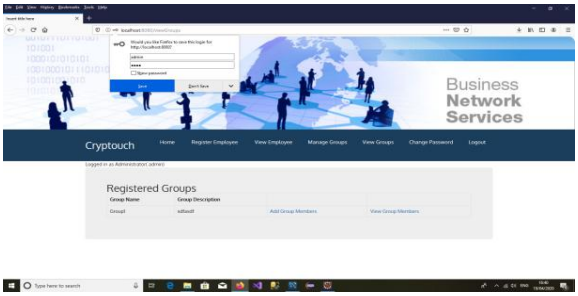
2. Authentication Page

One time password is sent on the registered email of employee or admin to authenticate the user.



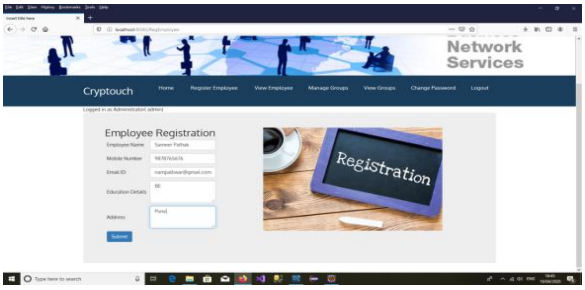
3. Admin Page

Once you have login successfully as an admin, this menu will appear from where admin can manage employees and groups.



4. Employee Registration

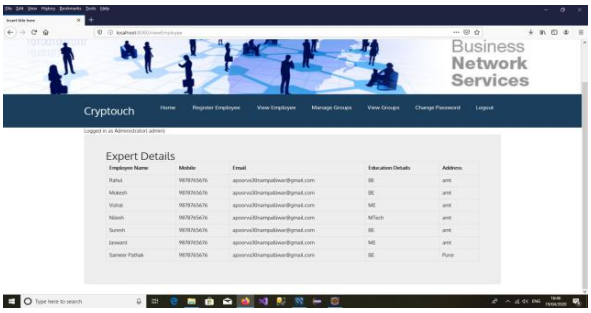
Admin will register new employee here with the proper credentials.



Once the employee is registered successfully, a mail is sent to the employee with the newly generated userid and password.

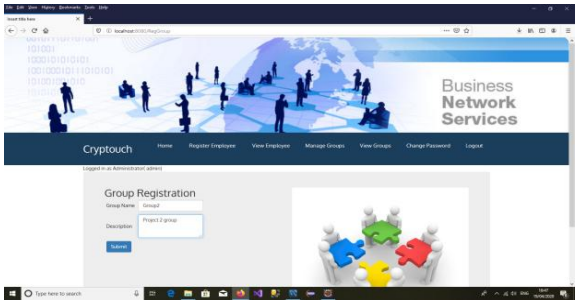
5. Employee Details

Here the list of employees with their details is shown to admin.



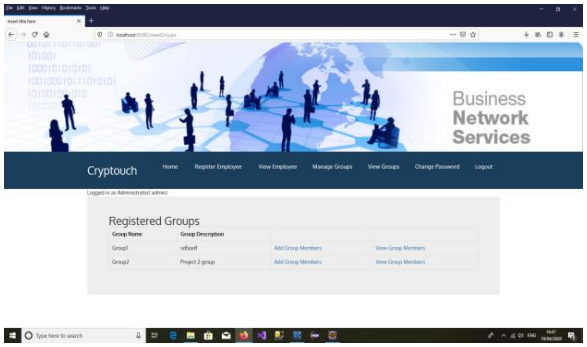
6. Group Registration

Admin can create the group and will specify the group name and its description.



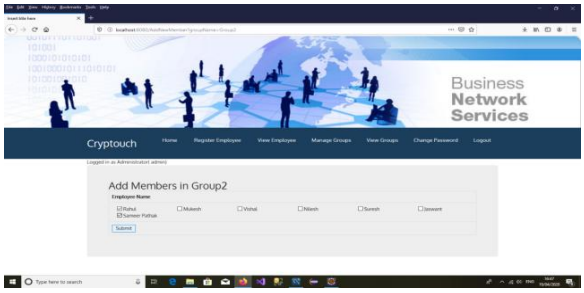
7. Group Details

Here the list of created groups is shown with the group name and its description, admin can also add or view the group members in any particular group.



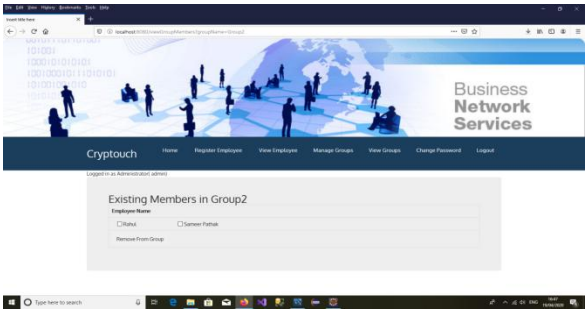
8. Add Member

List of registered employee is shown from where admin can add members in the selected group.



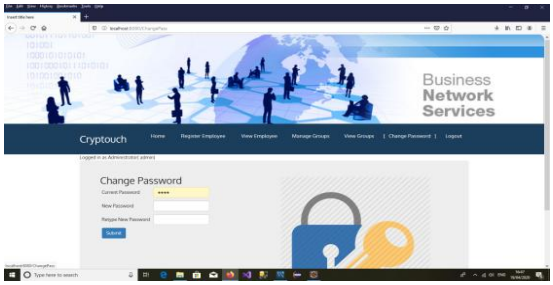
9. Manage Group

Here existing members in the group are given and admin can remove members from the group.



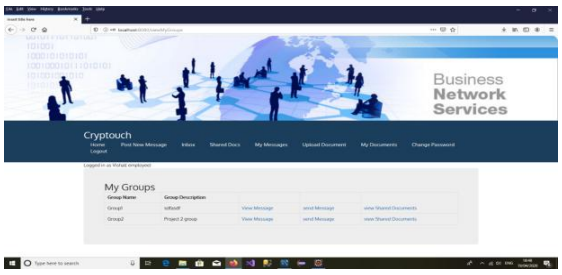
10. Change Password

Here admin can reset its password.



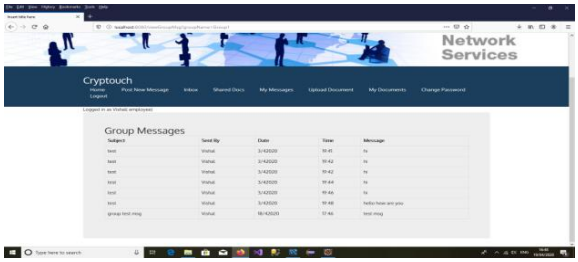
11. Employee Page

Once you have login successfully as an employee, this menu will appear from where employee can send/upload messages/files in group or to individual employee and can access shared documents or messages. And the group in which employee is added are shown here.



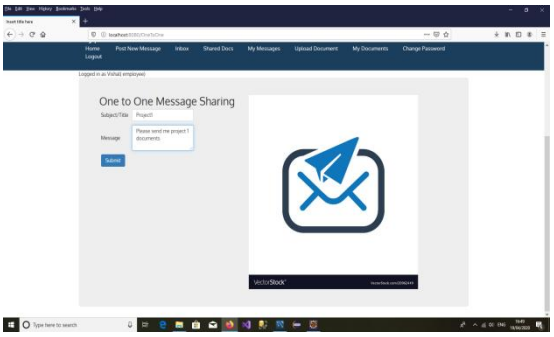
12. Inbox

This is the inbox where message shared within the group or to a particular employee are displayed with details.



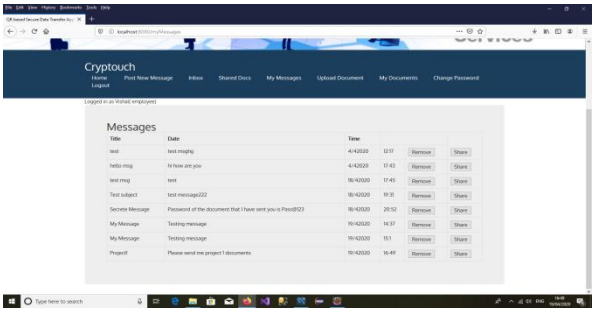
13. Post New Message

Here employee will post a text message with title which will get stored in messages section of employee and then it can be shared with other employees or groups.



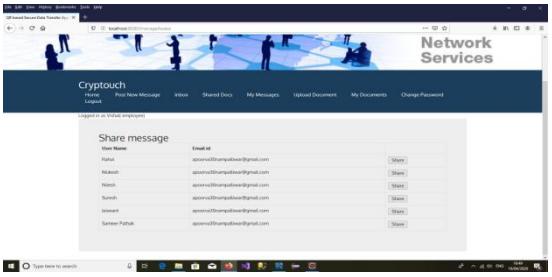
14. Messages

New messages posted by employee are stored here which the employee can further share or remove.



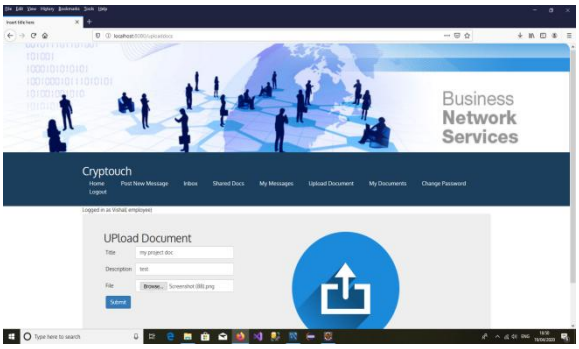
15. Share Messages

List of other employees with whom user can share messages are shown with their email id.



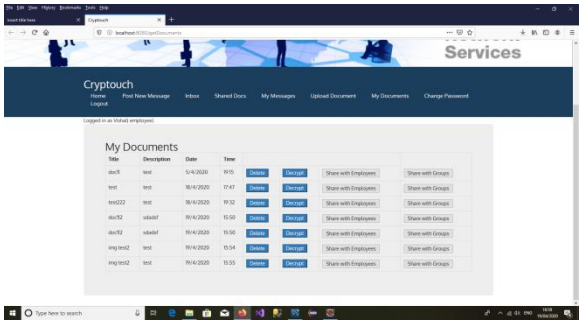
16. Upload Document

Employee will first upload a document here which he wants to share with title and description.



17. Documents

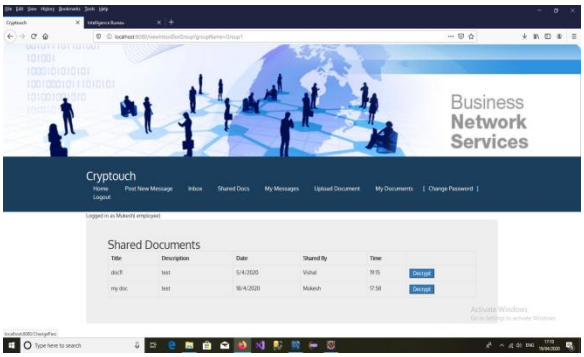
Uploaded document are stored here which can be delete, decrypt or shared within groups or other employees.



Here documents uploaded by employee Mahesh are shown.

18.Shared Documents

List of documents received by the employee is shown here with date, time and those who have shared it and which can be decrpyted.



VII. CONCLUSION

In this project we proposed communication system with blockchain technology. The documents will be maintained on IPFS server and the messages will be stored in blockchain network. We are storing the messages in encrypted format using AES algorithm. Other related data required to understand or leak the messages or documents will be maintained on application server.As we are keeping messages and related data on different servers, security of the system is improved.
Also we are using AES which is known as unbreakable algorithm.Therefore we can conclude that our communication system is unbreakable and secured from admin also.

REFERENCES

[1] Benet, J., “IPFS - Content Addressed, Versioned, P2P File System”, arXiv:1407.3561, 2014

[2] Karaarslan E., Akba¸s, M.F., ”Blockchain Based Cyber Security Systems” (Turkish), UBGMD Journal, Cilt 3, Sayı 2, Pages 16 - 21, DOI: 10.18640/ubgmd.373297,

[3] Vukoli´c, Marko. "The quest for scalable blockchain fabric: Proof-ofwork vs. BFT replication." International Workshop on Open Problems in Network Security. Springer, Cham, 2015.

[4] Dur˘gay Z., Karaarslan E., "Usage of Blockchain Technology in the E-Government Applications: Preliminary Study" (Turkish), Akademik Bili¸sim 2018, 2018

[5]Karl Wüst and Arthur Gervais, "Do you need a Blockchain?", IACR Cryptology ePrint Archive 2017 (2017): 375. [Online]. Available:https://eprint.iacr.org/2017/375