Innovation 2020
Organised by
Computer Engineering Department, Dr. D. Y. Patil School of Engineering, Lohegaon, Pune, Maharashtra, India in association with
International Journal of Scientific Research in Science, Engineering and Technology

Government Fund Distribution and Tracking System-Using Blockchain

Saket Sharma, Devendra Rathi, Raj Jaiswal, Farah Sayyed, Gourav Tiwari
Department of Computer Engineering, Dr. D. Y. Patil School of Engineering, Lohegoan, Savitribai Phule Pune University, Pune, Maharashtra, India

ABSTRACT

A blockchain is originally a growing list of records, called blocks that are linked by cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. By design, a blockchain is resistant to data modification. In this, we propose a system to track the funds allocated to the government as they travel through the government process at each stage. This system uses blockchain technology to maintain transparency and security at every stage as funds progress. This system allows to keep a clear record with all the users that are connected in the chain to carry out data transactions as necessary. The system uses encryption to secure transactional data using hashes to maintain a block of transactions in a way that is maintained and verified by each node involved to verify the transaction and save the data transparently within the government.
Keywords : Blockchain, Security, Transparency, Encryption, Government Funds, Cryptography.

I. INTRODUCTION

The world came to know about the Block-chain concept twelve years back when Satoshi Nakamoto conceptualized it in 2008; but it got developed a year later, using Bit-coin, a crypto-currency and digital payment system. The concept was later discovering to distributed ledger that leverages the block-chain to verify and store transactions without crypto-currency. The term block-chain is broadly used these days to represent a new disruptive technology poised to be the next big thing across industries from healthcare to finance to retail. According to Gartner, their client analysis on block-chain and related topics has quadrupled since August 2015.

A block-chain is a public ledger residing of ordered and time-stamped records of transactions arranged in data blocks which will use cryptographic validation to link themselves together. Block-chain is a path of recording data and transactions digitally. Each record is a block connected chronologically together into a chain. A block of one or more new transactions is composed into the transaction data part of a block. According to the approach of cryptography, digital signature generates a set of data information representing the identity and data integrity of the signer, usually appended to the data file.

Blockchain is touted for its potential to improve the trust and transparency of data- based transactions between individuals and organizations. The technology offers promise when strategically applied in the right contexts. But what are the conditions under which blockchain makes sense and how might the technology be useful when applied in government? Traditionally, organizations operating their own, individual IT systems seeking to collaborate must reckon with challenges including reconciliation of information, identifying a single source of truth, and facilitating accountability.

Blockchain technology addresses these challenges by providing a technical foundation that supports the execution of shared business processes in a way that no single entity controls the entire system. Government has an inherent need to build, sustain, and protect public trust in information and systems. In some situations, blockchain may help enhance this trust. Traditional relational database management solutions (e.g. Oracle and SQL), deployed globally across millions of applications, have one major operational constraint – the management of data is performed by a few entities who must be trusted. Distributed Ledger Technologies (DLT, commonly referred to as blockchain), an alternative architectural approach to managing data, and removes the need for a trusted authority to store and share a perpetually growing set of data. A foundational characteristic of a blockchain is trust. [Ref. 1]

II. PROJECT IMPLEMENTATION

Overview of Project Modules:

User upload the detailed information in word file .That file will encrypt with Advanced Encryption Standard algorithm that takes plain text and private key and encrypt data. Encrypted data will store on node. Also hash value of uploaded file will store. Authority will see the file after login and send request to get the file .Key Manager will send the key on Authority mail. Then authority will enter the key and will get the decrypted file from node. Before getting the file, data auditing will perform by checking hash value of already stored data on node. Similar process will be followed by each and every module (i.e. User, Authority, and Government) included in this process. Key Manager is used here to provide the encrypted and decrypted key. Here they will also delete his file from node and also get file from node. Data will store on different node through block chain concept. [Ref.2,3,6,10,]

User

- User registers to the system
- User login to the system
- User can view profile
- User will upload file
- User can view details
- User can access the data
- Lastly, logout from the system.

Authority

- Authority registers to the system
- Authority login to the system
- Authority can view profile
- Authority will upload file
- Authority can view details
- Authority can view the data
- Lastly, logout from the system.

Government

- Government registers to the system
- Government login to the system
- Government can view profile
- Government can view details
- Government can view the data
- Lastly, logout from the system.

III. LITERATURE SURVEY

TABLE I. LITERATURE SURVEY TABLE

Sr. No.	Paper Name	Author	Journal	Description
1.	"Logistics and Supply Chain Management: Exploring the Mindful Use of a New Technology	Tino T. Herden	IEEE on 2018	advancement of the theory of mindfulness to assess the use of block-chain technologies in the context of logistics and supply chain management. Several implications, both on the theoretical and on the managerial levels, can be deduced from the case study discussion
2.	Blockchain for Supply Chain Management: Architectural Elements and Challenges Towards a Global Scale Deployment	Varvarigou	IEEE on 2017	blockchain fit in the supply chain industry. It defines the specific elements of blockchain that affect the supply chain such as scalability, performance, consensus mechanism, privacy considerations, location proof and cost
3.	An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends	Zibin zheng, hong-ning dai	2017 IEEE 6th International Congress on Big Data	Gives an overview of blockchain technologies including blockchain architecture and key characteristics of blockchain. This paper then discusses the typical consensus algorithms used in blockchain.

4.	Blockchain and Its Applications – A Detailed Survey	Supriya Thakur Aras, Vrushali Kulkarni	International Journal of Computer Applications (0975 – 8887) Volume 180 – No.3, December 2017	Different applications of blockchain- such as fund transfer, digital contract, education and medical industry. Limitations in block chain technology and the ethics of crypto currency.

IV. Hardware Interfaces

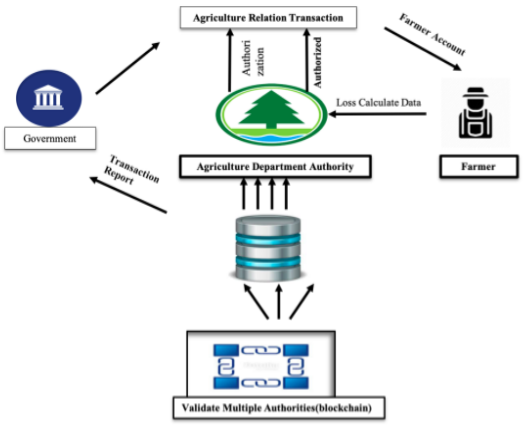
Processor - Dual core/Intel i3
Speed - 1.8 GHz
RAM - 2 GB (Min)
Hard Disk - 100 GB
Key Board - Standard Windows Keyboard
Mouse - Two or Three Button Mouse
Monitor /LCD - SVGA/LED

V. Software Interfaces

Operating System - Windows
Application Server - Apache Tomcat 7
Front End - HTML, JSP, CSS
Scripts - JavaScript.
Database - My SQL 5.0
IDE - Eclipse Oxygen
Coding Language - Java 1.8

VI. SYSTEM DESIGN

A. System Architecture



B. Mathematical Model

Let us consider S as a system for Government Fund Tracking System.
S=
INPUT:
Identify the inputs
F= f1, f2, f3 ..... FN— F as set of functions to execute commands.

I= i1, i2—I sets of inputs to the function set
O= o1—O Set of outputs from the function sets,
S= I, F, O
I = Input given by the user.
O = Output i.e. tracked location.
F = Functions implemented to get the output
Space Complexity:
The space complexity depends on Presentation and visualization of discovered patterns.
More the storage of data more is the space complexity.
Time Complexity:
Check No. of patterns available in the datasets= n
If (n (1)) then retrieving of information can be time consuming.
= Failures and Success conditions.

Failures:

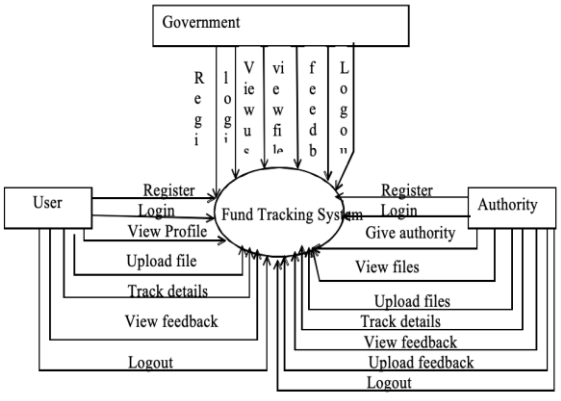
- Huge database can lead to more time consumption to get the information.
- Hardware failure.
- Software failure.

Success:

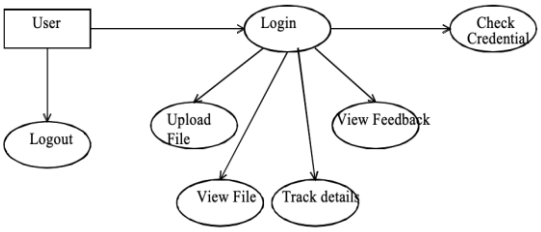
- Search the required information from available in Datasets.

A. Data Flow Diagram

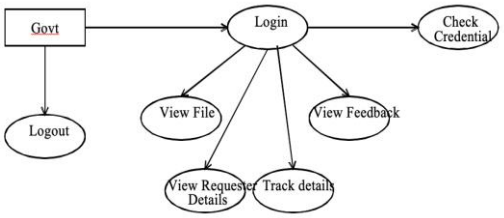
DFD 0



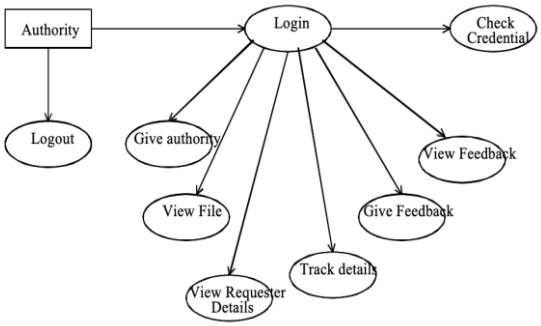
DFD1



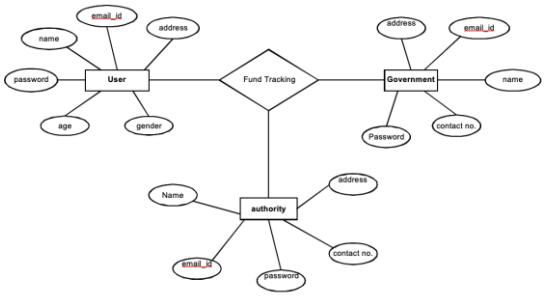
DFD2



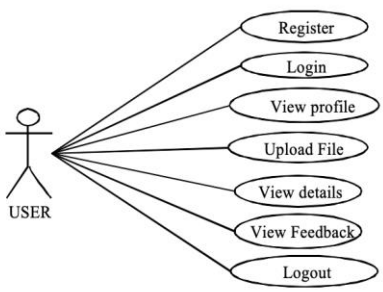
DFD 3

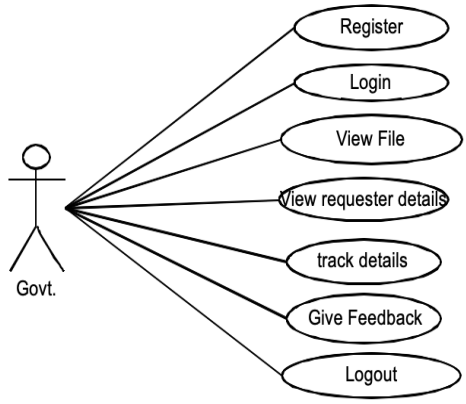


A. ER diagram:



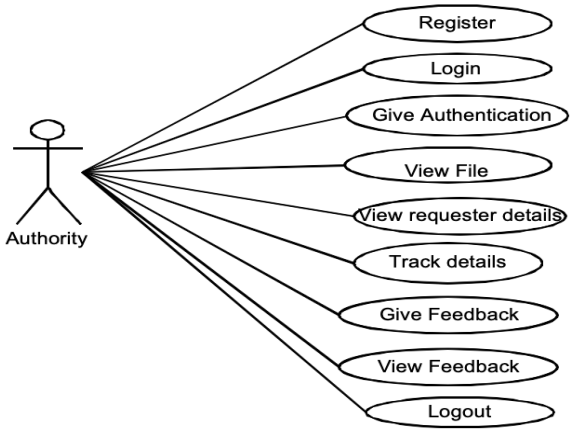
B. Usecase Diagram:



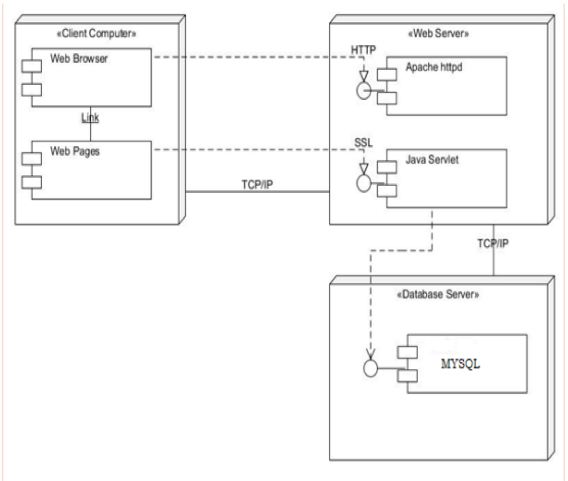


System identifies the customer as “Woman”

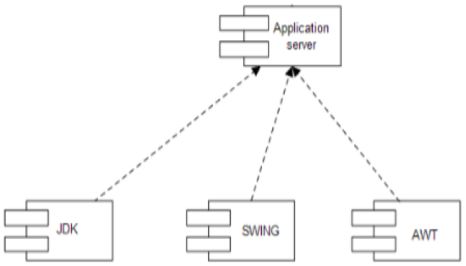
In the above screen the system identifies the customer as “Woman”



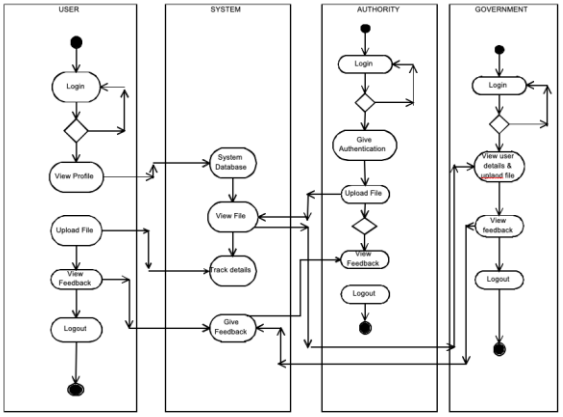
C. Deployment Diagram:



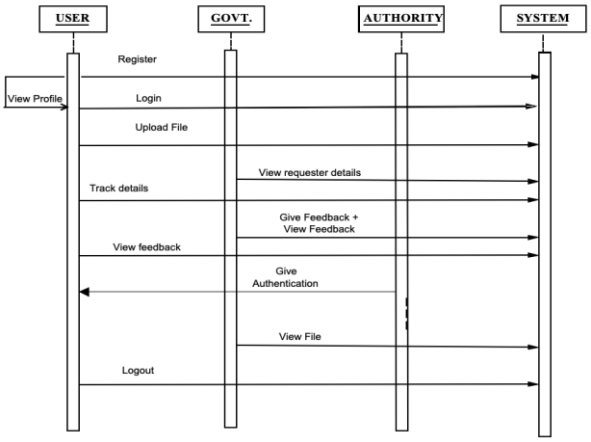
D. Component Diagram:



E. Activity Diagram



F. Sequence diagram:



VII. Algorithm Details:

In this we are going to increase the security and time efficiency by using algorithms i.e. Block-chain Algorithm (Cryptography algorithm).

The main purpose of using public-key cryptography for the blockchain is to create a secure digital reference about the identity of a user. Secure digital

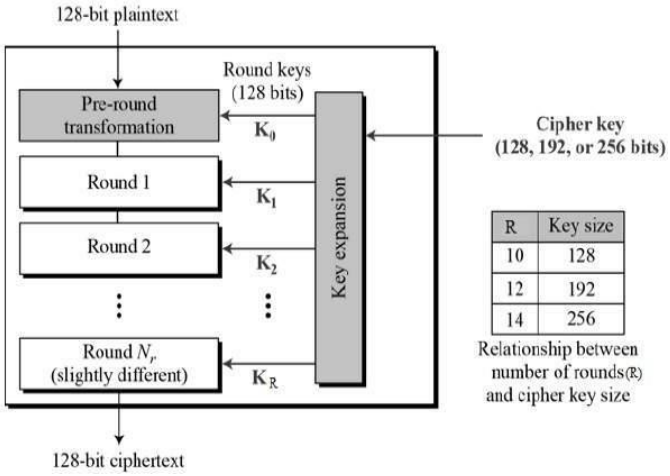
references about who is who, and who owns what, are the basis for P2P transactions. Public-key cryptography allows proving one's identity with a set of cryptographic keys: a private key and a public key.

VIII. Advanced Encryption Standard

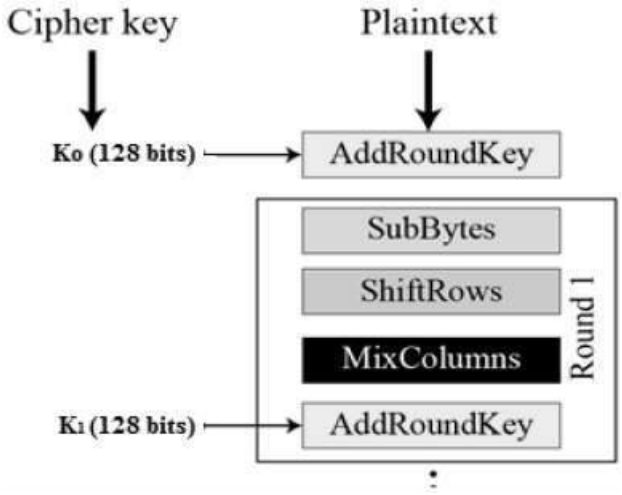
The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six times faster than triple DES.
The features of AES are as follows –

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

The schematic of AES structure is given in the following illustration –



Encryption Process: Here, we restrict to description of a typical round of AES encryption. Each round comprises of four sub-processes. The first-round process is depicted below –



Byte Substitution (Sub Bytes): The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

Shift rows: Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. [Ref. 2,3,6]

IX. SHA-1(Secure Hash Algorithm):

Secure Hashing Algorithms, also known as SHA, are a family of cryptographic functions designed to keep data secured. It works by transforming the data using a hash function: an algorithm that consists of bitwise operations, modular additions, and compression functions. The hash function then produces a fixed size string that looks nothing like the original. These algorithms are designed to be one-way functions, meaning that once they're transformed into their respective hash values, it's virtually impossible to transform them back into the original data. A common application of SHA is to encrypting passwords, as the server side only needs to keep track of specific user's hash value, rather than the actual password. [Ref. 12,13]

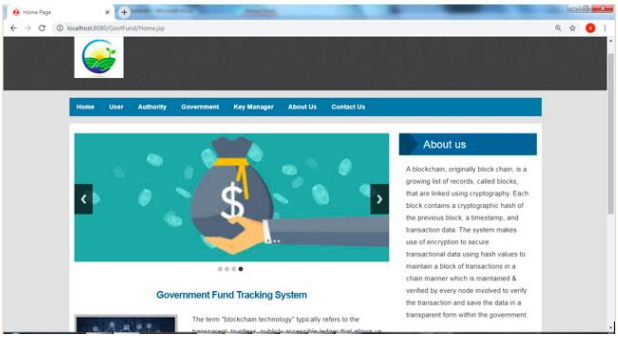
X. RESULTS

Outcomes:

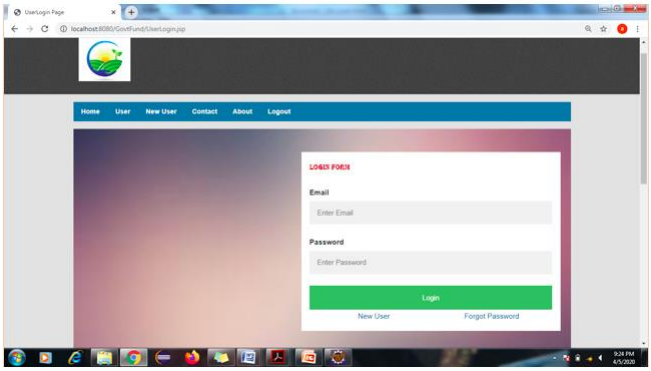
The application will be able to analyse the data from various different internet sources and help in determining a pattern among the fraud or scam occurred in various regions thereby predicting future fraud regions and type of crime in these regions also it may help law enforcers to generate criminal profile as per the crime type and region. The system will speed-up the fraud analysis process and digitizes it so that multiple organizations can benefit from this system at the same time. Such a system may help the law enforcers to reduce frauds by deploying resources effectively and preventing criminals from committing crimes thereby providing security to citizens

Screenshots:

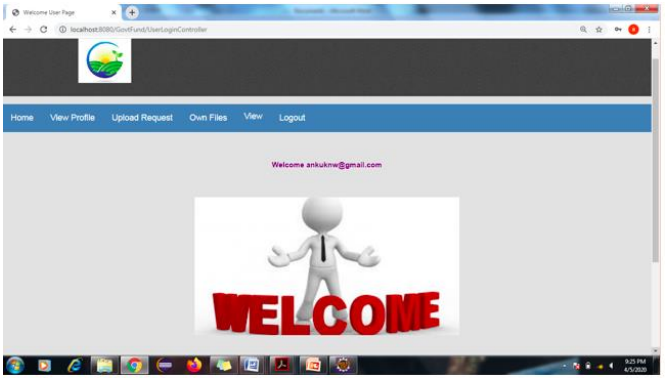
1. Home page: -



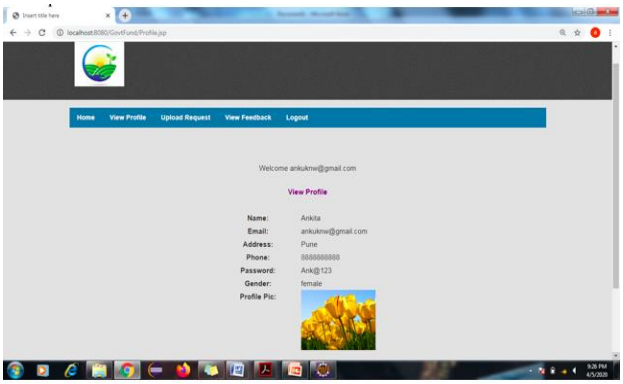
2. Login form: -



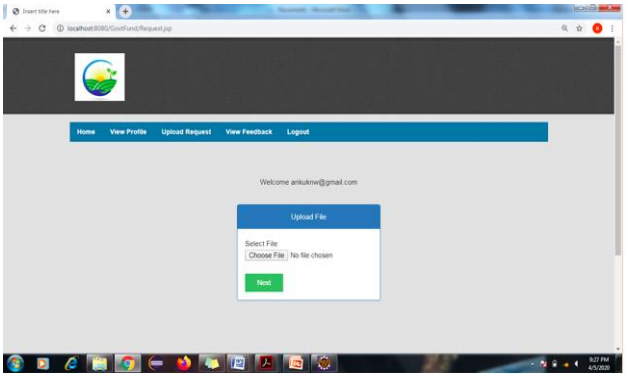
3. After Login Welcome Page: -



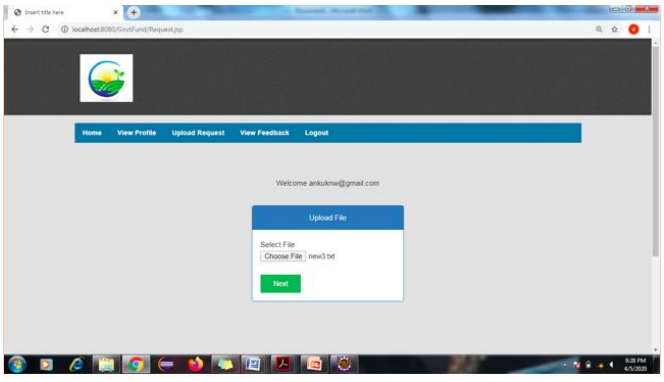
4. View Profile: -



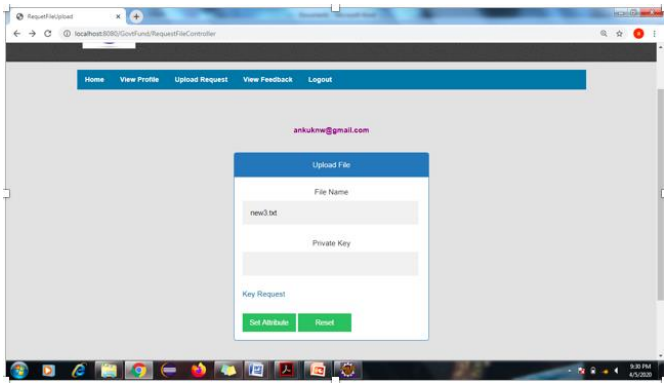
5. Upload Request: -



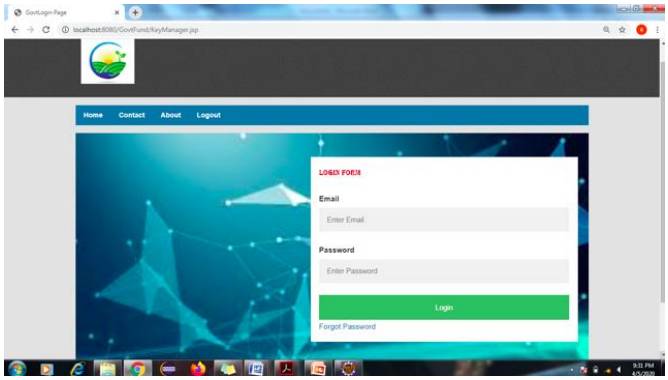
6. File Select for Uploading: -



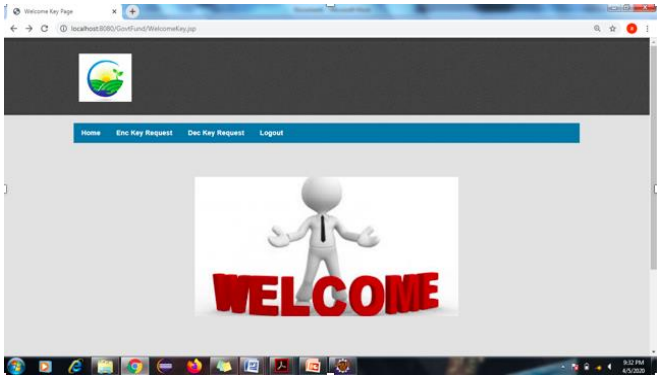
7. Send Key Request: -



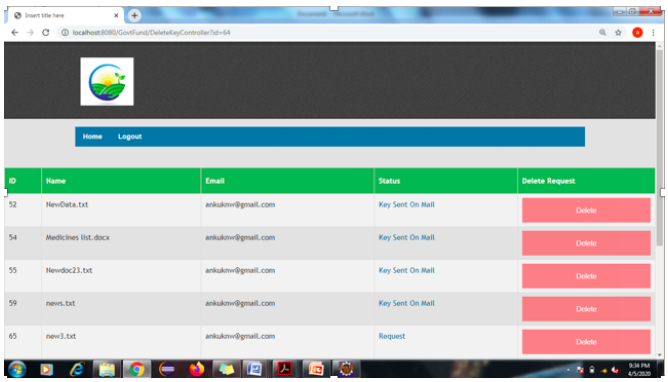
8. Key Manager Login Form: -



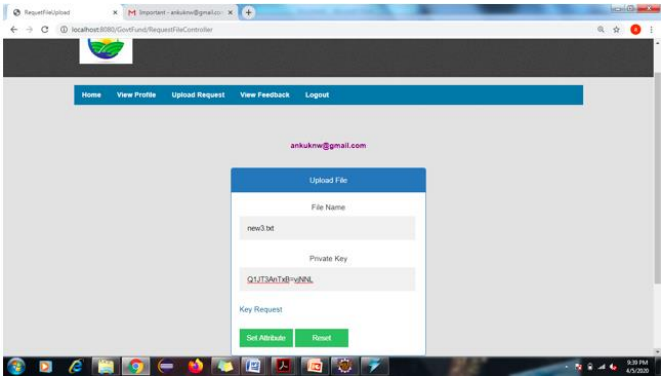
9. After Login: -



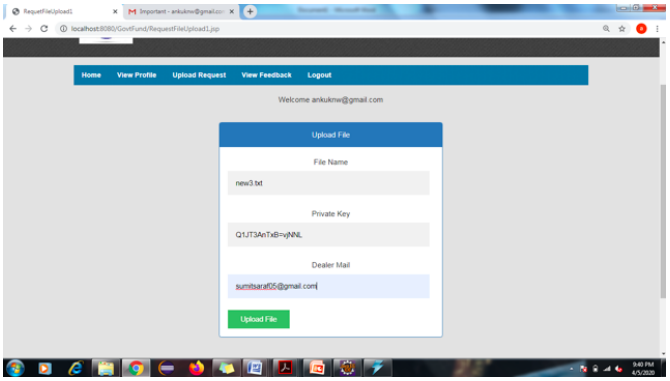
10. Encryption Key Request: -



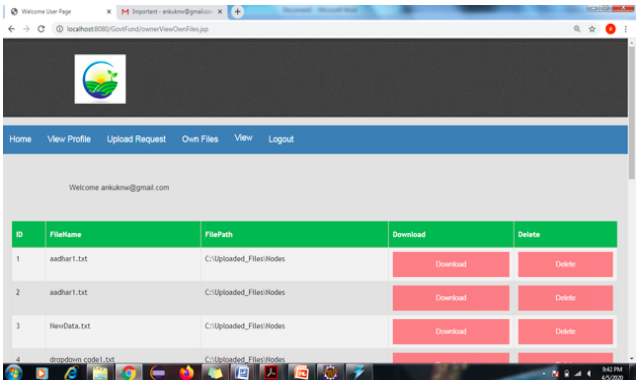
11. Enter key which is sent on the email id: -



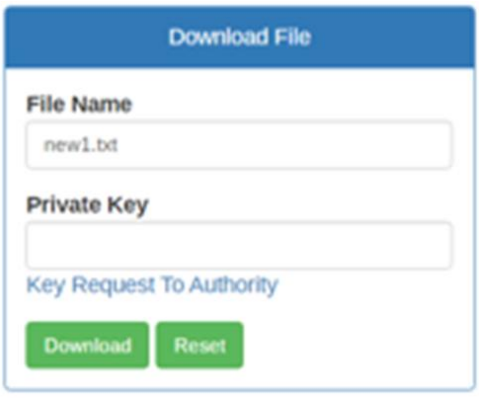
12. Next page enter email id to which file will be sent and upload it.



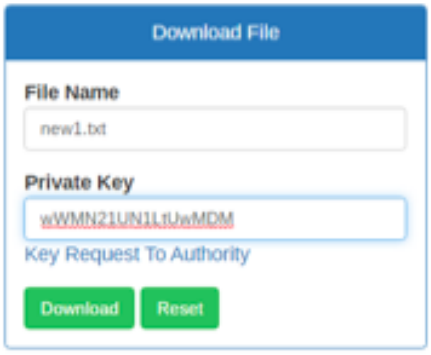
13. View files to download



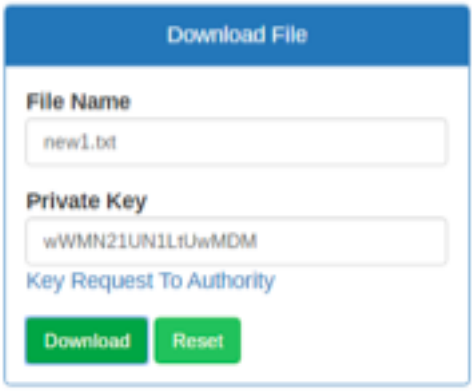
14. When click on download



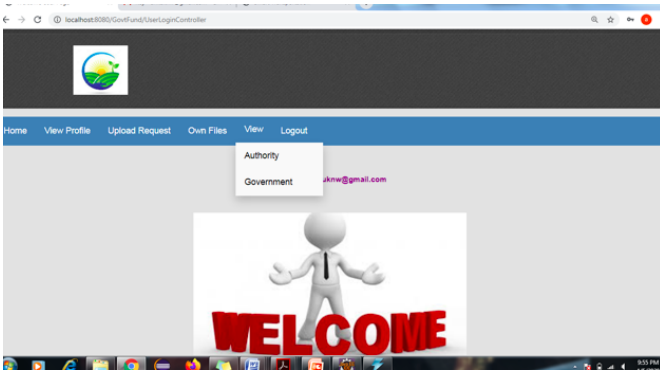
15. Enter key to download file



16. Click on download then file will be downloaded



17. View Details:



18. Next page show list of users

XI. CONCLUION

When considering building blockchain applications, we also have to consider the access and privacy challenges. Then, with other additional improvements, this blockchain model can provide transparency in all government transactions, without any discrepancy. Due to the decentralized ledger, all transactions can be verified and cannot be modified. The money that is released can be tracked, and anyone can find out how it is being used. Such a blockchain will surely reduce the prevalent corruption in this country and create a huge positive impact on its economic development.

XII. ACKNOWLEDGEMENT

It gives us a great pleasure in presenting the paper on “Government Fund Distribution and Tracking system”. We would like to thank Prof. Gourav Tiwari, Computer Engineering Department, DYPSOE, Pune for giving us all the help and support we need during course of the Paper writing work. We are really grateful to him. Our special thanks to Prof. Monika Dangore, Project Coordinator who motivated us and created a healthy environment for us to learn in the best possible way. We also thank all the staff members of our college for their support and guidance.

XIII. REFERENCES

[1]. Jiafu Wan, Jiapeng Li, Muhammad Imran, Di Li, Fazal-e-Amin, “A Blockchain-Based Solution for Enhancing Security and Privacy in Smart Factory”,IEEE Transactions on Industrial Informatics Volume: 15, June 2019.

[2]. Antonios Litke, Dimosthenis Anagnostopoulos, Theodora Varvarigou, “Blockchains for Supply Chain Management: Architectural Elements

and Challenges Towards a Global Scale Deployment", MDPI January 2019.

[3]. Mrs. R.Meenatkshi , Mrs. K.Sivaranjani, "A Comparative Study on Fraud Detection in Financial Statement using Data Mining Technique", International Journal of Computer Science and Mobile Computing, Vol.5 Issue.7, July- 2016, pg. 382-386.

[4]. Analysis KK Tangod, GH Kulkarni, "Detection of Financial Statement Fraud using Data Mining Technique and Performance",International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 7, July 2015 .

[5]. Chi Harold Liu, Senior Member, IEEE, Qiuxia Lin, Shilin Wen. "Blockchain-enabled Data Collection and Sharing for Industrial IoT with Deep Reinforcement Learning", IEEE Transaction on Industrial Volume: 15, Issue: 6 , June 2019

[6]. Apoorva Mohite, Ajay Acharya, "Blockchain for government fund tracking usingHyperledger", IEEE Transactions on Fuzzy Systems, April 2018.

[7]. Ning Wang, Jing-Chao Sun, Meng JooEr,"Tracking-Error-Based Universal Adaptive FuzzyControl for Output Tracking of Nonlinear Systemwith Completely Unknown Dynamics" ,IEEEAPRIL 2017.

[8]. Adam Ghandar, Zbigniew Michalewicz, Ralf Zurbruegg, Chee Cheong,"Index Tracking Fund Enhancement Using Evolving Multi-CriteriaFuzzy Decision Models",IEEE Congress on Evolutionary Computation.

[9]. Shangping Wang, Dongyi Li, Yaling Zhang, Juanjuan Chen, "Smart Contract-Based Product Traceability System in the Supply Chain Scenario", IEEE Access, 2019.

[10]. M. Nakasumi, "Information Sharing for Supply Chain Management Based on Block Chain Technology," in 2017 IEEE 19th Conference on Business Informatics (CBI), Thessaloniki, Greece, Jul. 2017.

[11]. M. Kim, B. Hilton, Z. Burks, and J. Reyes, "Integrating Blockchain, Smart Contract-Tokens, and IoT to Design a Food Traceability Solution," in 9th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Univ British Columbia, Vancouver, Canada, Nov. 2018.

[12]. Z. Li, H. Wu, B. King, Z. Ben Miled, J. Wassick, and J. Tazelaar, "A Hybrid Blockchain Ledger for Supply Chain Visibility," in 2018 17th International Symposium on Parallel and Distributed Computing (ISPDC), Geneva, Switzerland, Aug. 2018.

[13]. T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains everywhere - a use-case of blockchains in the pharma supply-chain," in 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, Jul. 2017.

[14]. X. Ye, Q. Shao, and R. Xiao, "A supply chain prototype system based on blockchain, smart contract and Internet of Things," Science & Technology Review, vol. 35, no. 23, pp. 62–69, 2017.