A Synopsis on

Enhancing Data Security in Cloud using Blockchain

Submitted in partial fulfillment of the requirements
of the degree of

Bachelor of Engineering

in

Information Technology

by

Dhananjay Yadav (17204015)
Aditi Shinde (16104022)
Akash Nair (16104051)

Prof. Kiran Deshpande
Prof.Sneha Kanchan

Department of Information Technology
G.B. Road , Kasarvadavli, Thane(W), Mumbai-
400615 UNIVERSITY OF MUMBAI
2019-2020

CERTIFICATE

This is to certify that the project Synopsis entitled ***"Enhancing data security in Cloud using Blockchain"*** Submitted by ***Dhananjay Yadav (17204015)***, ***Aditi Shinde (16104022)*** and ***Akash Nair (16104051)*** for the partial fulfillment of the requirement for award of a degree ***Bachelor of Engineering*** in ***Information Technology*** to the University of Mumbai, is a bonafide work carried out during academic year 2019-2020

(Prof. Kiran Deshpande)
Guide

(Prof.Sneha Kanchan)
Co-Guide

Prof. Kiran Deshpande
Head Department of Information Technology

Dr. Uttam D.Kolekar
Principal

External Examiner(s)

1.

2.

Place: A.P. Shah Institute of Technology, Thane
Date:

Declaration

I declare that this written submission represents my ideas in my own words and where others' ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

—————————————————

(Signature)

—————————————————

(Dhananjay Yadav 17204015)
(Aditi Shinde 16104022)
(Akash Nair 16104051)

Date:

Abstract

Cloud computing is the protracted revelation of computing as effectiveness, where data owners can remotely store their data. The essential service presented by the Cloud is Data Storage. On the other hand, it is a tricky task for sharing data in multi-owner manner anywhere group admin and all group members can store and alter data while protecting data and identity privacy from associate un-trusted cloud server, due to the frequent change of the membership. So secure multi-owner data sharing scheme for dynamic groups in the cloud computing have been projected which absorb addition of group signature and broadcast encryption techniques. However, this method additionally recognized some boundaries in terms of competency and security. since multi-owner data storing and sharing in dynamic surroundings dumps enormous amount of data files in the cloud, which leftovers in cloud for imprecise period of time. The confidential information stored may be changed by service providers. To maintain cloud file's security and privacy regular elimination of unwanted files is required. To determine this draw- back, we propose new framework which is Reliable and Scalable Secure Method to Store and Share Secrete Data for groups and individuals in cloud using blockchain.

Introduction

In past years, the recent boom of cloud storage services makes it easier than ever for cloud users to share data with each other. To ensure users' confidence of the integrity of their shared data on cloud, a number of techniques have been proposed for data integrity auditing which focuses on various practical features, e.g. The support of fluid data, public auditing with integrity, low computational cost, low storage overhead. However, most of these techniques consider that only the original data owner can modify the shared data, which limits these techniques to client read- only applications. More over usage of blockchain in this architecture will result in a situation where an adversary cannot get anything about the raw users file data from the blockchain, as only URLs and hash values are stored in it. Recently, a few researches have started regarding more realistic scenarios by allowing multiple cloud users to write data without loss of integrity. None the less, these attempts are still far from being practical due to the vast computational cost on cloud hardware, especially when error detection possibility is required by the system. We propose an integrity write scheme for cloud data sharing services summarized by multi-user modification on data that's stored on cloud. Our scheme can resist impersonation attacks, which is not considered in existing techniques that support multi-user modification.

Objective

Following are the major objectives provided by our system:

- To provide effective security to the data stored on cloud using blockchain.

- To maintain better integrity of data on cloud as the hash values can be compared with original file.

- To avoid fraudulent of data as permission from both the user and the owner is required to make any changes.
- To have the consensus mechanism for the cloud group users as blockchain works on the mechanism where consent from all the owners is required to add a block or change any data.

- Restricting unauthorized access to files as even after been successful in downloading the file attacker/hacker will only get hash values or URL’s

Literature Review

The papers referred are mentioned below:

[1] Nakamoto S . Bitcoin: A peer-to-peer electronic cash system[J]. Consulted, 2008.

- A Blockchain, originally block chain refers to the growing list of records or data in a chain like manner. The blockchain was found in 1992 as a technology to cease the tampering of timestamp on files. The latest technology blockchain can be traced back to 2008 when Satoshi Nakamoto (along with his colleagues) revised blockchain into a ledger like continuous trans- action list which later led to the founding of the first cryptocurrency called bitcoin. Bitcoin was the first currency to have blockchain backing it for its secure and tamper less transaction which led to cryptocurrency gaining a new advancement and boon to its use in today's date. Blockchain process involves breaking down transaction data into chunks or blocks of a sort which has three main parts that include data, previous hash and its own hash that has been generated by the hash of previous blocks hash and the blocks data. Any tampering to the block leads to the change in the hash values and which in turn leads the hash in the previous block to be untraceable. This makes the blockchain very useful to use in transaction and monetary related functions. The data in the block may include transaction details like sender, receiver, amount, ID etc. The blockchain technology seemed promising at first because of its high level of security that it provides but the cost and complexity of installing it was very high. It wasn't possible to implement it everywhere because of its high perpetuity, complexity and network cost that comes with it. Hence the use of blockchain was limited to the cryptocurrency since it had a high risk while transactions because it's conducted through the network. The timestamp server would broadcast the hash of which the block was added or any changes were made, this proves that the block was made and it'd be relevant to get into the hash of the block. Each timestamp includes the timestamp of the previous block in hash format which led to taking the data and the timestamp hash as the input for the new block that is to be generated. This leads to the re-enforcing the previous block by the new block that is created with the timestamp. They have proposed a system for electronic transactions without relying on trust also started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double spending. To solve this, they proposed a peer-to peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. We will try to implement the framework they used for coins in our data on the cloud.

- Advantages:

Provides a secure means of transaction with lowest possible chance of risks involved with tampering. Calculating hash would require a lot of effort.

- Disadvantages:

Requires a good network speed and is not as cost effective when it comes to transactions. Its also complex to be implemented.

[2] 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI) Amita Kashyap, G. Sravan Kumar, Sunita Jangir, Emmanuel S. Pilli, Preeti Mishra "IHIDS : Introspection- Based Hybrid Intrusion Detection System in Cloud Environment".

- Cloud Computing delivers on-demand and pay-as-you use service to users with less service provider interaction which seems great, but also increases the threat of cyber-attacks. Every year, several organizations report events of attacks. For example, an Annual Security report from Cisco shows that the Boston Marathon bombing made up 40 percent of the spam messages sent across the world and ENSIA reported attack on Dropbox by Distributed Denial-of-Service (DDoS) which affected the 15 hrs. of functionality and Amazon cloud also infected with DDoS botnets and many more attacks every year. Various common attacks, in turn, causes confidentiality, security and integrity issues to cloud services and resources. Some of the common attacks are DDoS attacks, backdoor channel attack, flooding attack, port scanning attack, a user to root attack, an attack on VM or hypervisor and many more. To prevent or to get notice of such attacks an Intrusion detection system was implemented in the hypervisor layer of the cloud which led to notification of any or all types of attack on the cloud. The pros of including an IDS in the hypervisor include detection of any insider or outsider attacks. Any kind of intrusion attempts led to the cloud owner and admin getting the notification related to it. This made the system secure and led to possibility of immediate counter against the attacker. The one major flaw with including an IDS at hypervisor layer was that the IDS only notified and

- Advantages:

Notifies all unnatural activities to the cloud admin and also notifies internal or external attacks since all data passes through the hypervisor layer.

- Disadvantages:

IDS only notify the infiltration; it doesn't lock it. Hence, at times it would be too late before the user or admin is notified.

[3] Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., Kishigami, J. J. (2015). Blockchain contract: A complete consensus using blockchain. 2015 IEEE 4th Global Conference on Consumer Electronics (GCCEP).

- In this referred paper the actual concept was to provide a consensus mechanism to the data in which the publisher specifies that the mechanism was used to provide consensus mechanism to the data which is referred as contract data. A tremendous number of contractual documents, such as those relating to "purchase and sale agreement", "deed of assignment" and "license agreement", are created every day all over the world. Computers build it potential to record and manage these documents simply. However, they are harder to protect for a longer duration of time and to verify in later years because computer records are quite easy to change. We believe that blockchain technology has great potential for use in recording a trail of consensus. This is as a result of the blockchain itself is robust against attack, anyone will verify its records, and it's troublesome to vary its history. Hence the blockchain was implemented to have a contract transaction so secure that no data can be tampered or retrieved if attacker tries it so. The contract is divided in part of two where the mediator and contractors have a complete say in the part of contract. The contract is divided so that the data or address of the destination contractor, contract information, and the sender contractor information is all stored in hash values and sent over the network. The receiver contractor accepts and then the contract is sent back the first contractor to verify and which is then forwarded to the contract mediator who then confirms the contract which is then settled. This allows a complete trust and confidentiality between the contractors and mediator. It was one of the best ways of having an online transaction or contract which provided utmost security and anonymity to the contractor. The technology provided anonymity to the contractors which was itself a pro and a con. The anonymity implies that the data and information on the contractors remained unscathed and no information was leaked while the contract was in progress and no type of attack would breach the security of information, This was also a flaw in the system because the anonymity of the contractors means there is a possibility of fraudulent by the unknown contractors and it would be unable to trace them because the system itself maintains the anonymity of the contractors. The referred paper explains the consensus mechanism through an example of contract between 3 members dealing with a contract.

- Advantages:

The parties involved in the contract might be anonymous because of blockchain. This helps keep the information from being overuned in the cyberspace.

- Disadvantages:

The consensus mechanism consumes a lot of resources, hence its hefty to be used. The anonymity because of blockchain is also a concern when dealing with the cyber fraudery.

Problem Definition

In current scenario cloud security is good but after a certain extend can be compromised, in order to overcome such a scenario, we are providing an extra layer of security to the cloud data using blockchain. Providing blockchain to data will ensure better security on the cloud servers thus providing secure means of data transmission.

Proposed System Architecture/Working

To address the issue, we propose an architecture where the front end would be a web-based interface where most of the interaction between the user and the cloud happens. The cloud automation layer comes next and then comes the blockchain layer where most of the secure policies are implemented. The web interface allows the user to upload or download data on cloud. Once the data is uploaded on cloud the data is then forwarded to the cloud automation layer which allows the system to know what kind of data is being stored on cloud. The data that is then directed to the blockchain layer which performs various functions on cloud. The few functions that the cloud performs are dividing data into chunks or blocks, applying cryptography and creating and linking blocks with hash values using hash pointers. Once the chain of block is created it is then forwarded to the cloud storage service. We are using Cloud service, which provide immediate storage and retrieval of data. The decryption of data will happen in the same opposite way as that of encryption which would allow the user to download his/her data. Our system would also have consensus mechanism for multi-user network where if someone wants access to your files or anybody tries to access the data you have uploaded with ill intent you will get a notification regarding the same. The consensus mechanism allows user to store data on the platform without having second thoughts about the security of data on the cloud. Even the privileged users cannot access the data of the users without consent of the users.

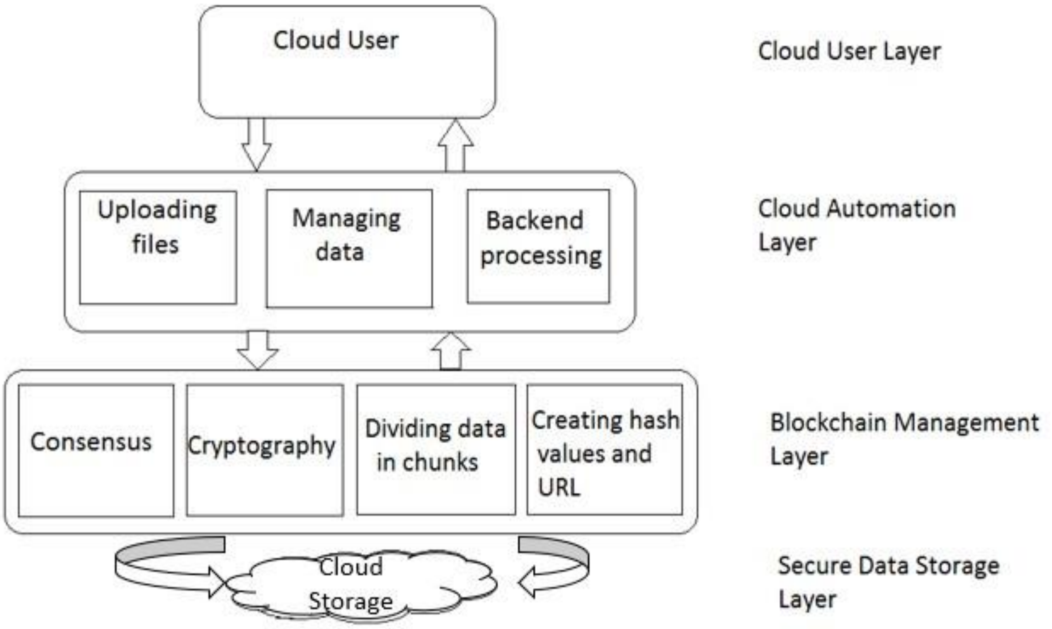

Figure 1: Proposed System Working

The working of the project would go as follows, the user would first need an account and account will be created by authorized personnel of the organization using the platform. Once created the account the user would log in and upload his/her data on the platform where he intends to put it. There are different levels of access of data such as Private, Public and Group. After uploading the data, the data is then processed and secured using an encryption algorithm and then pushing the data onto the cloud itself. The data before being accessed by anyone else would have a blockchain consensus protecting it, which would require the users consent to access the data. This allows proper storage and secure way of sharing and storing data.

Design and Implementation

Block diagram

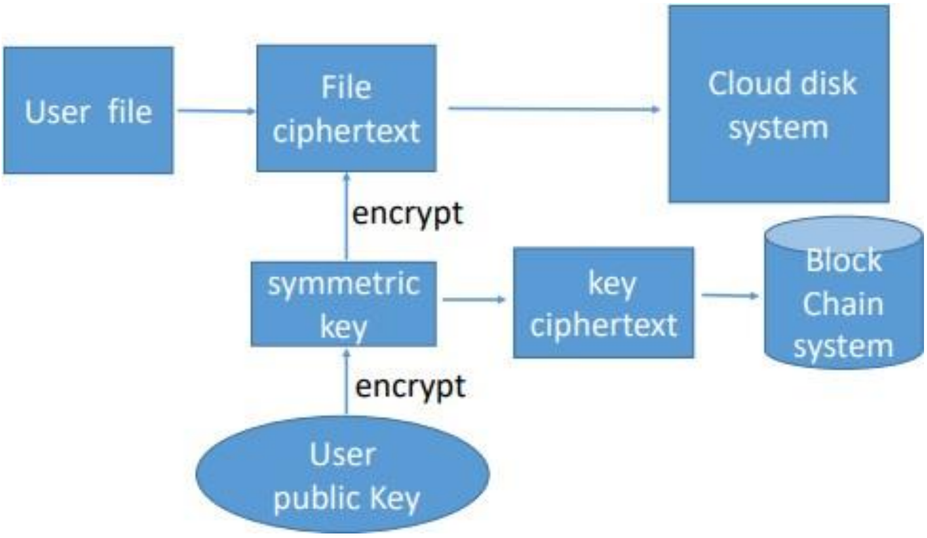

Figure 2: Block diagram

Use case diagram

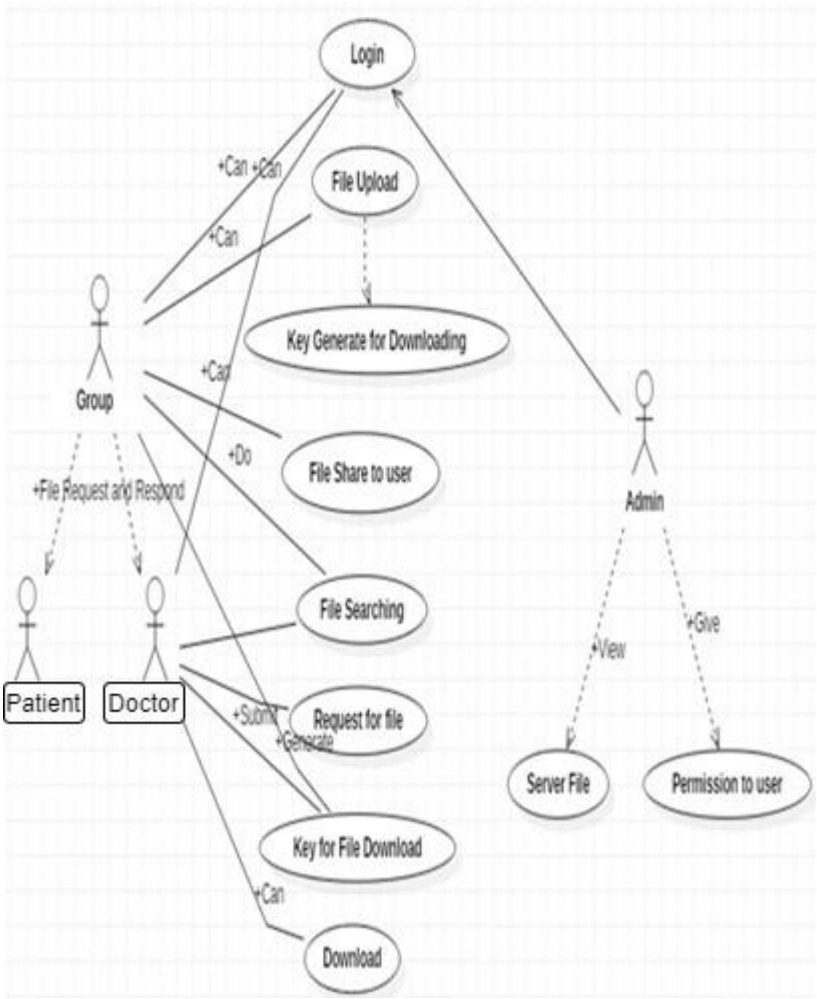

Figure 3: Use case diagram

Data Flow diagram

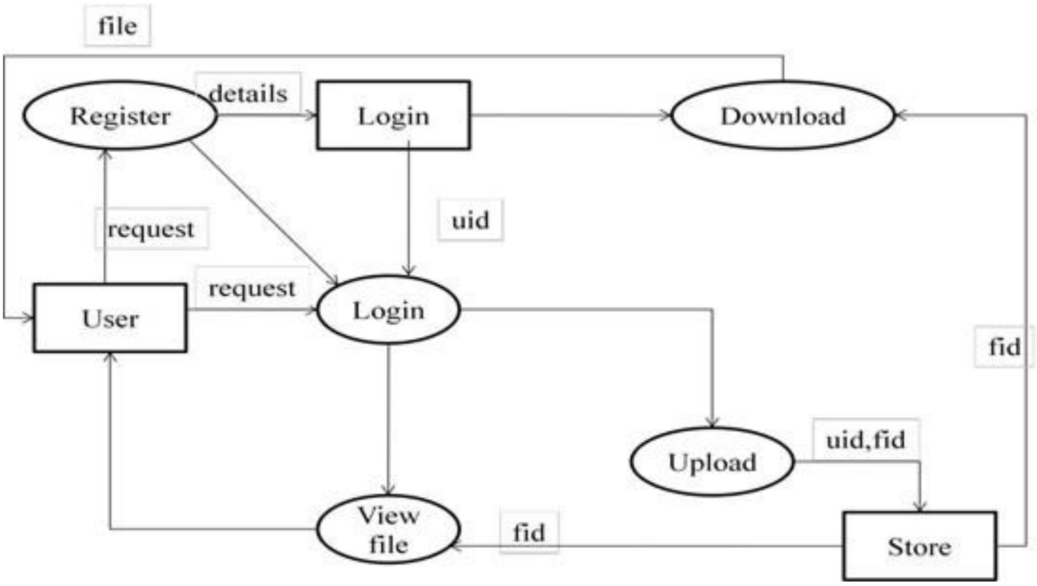

Figure 4: Data flow diagram

Detail Data Flow diagram

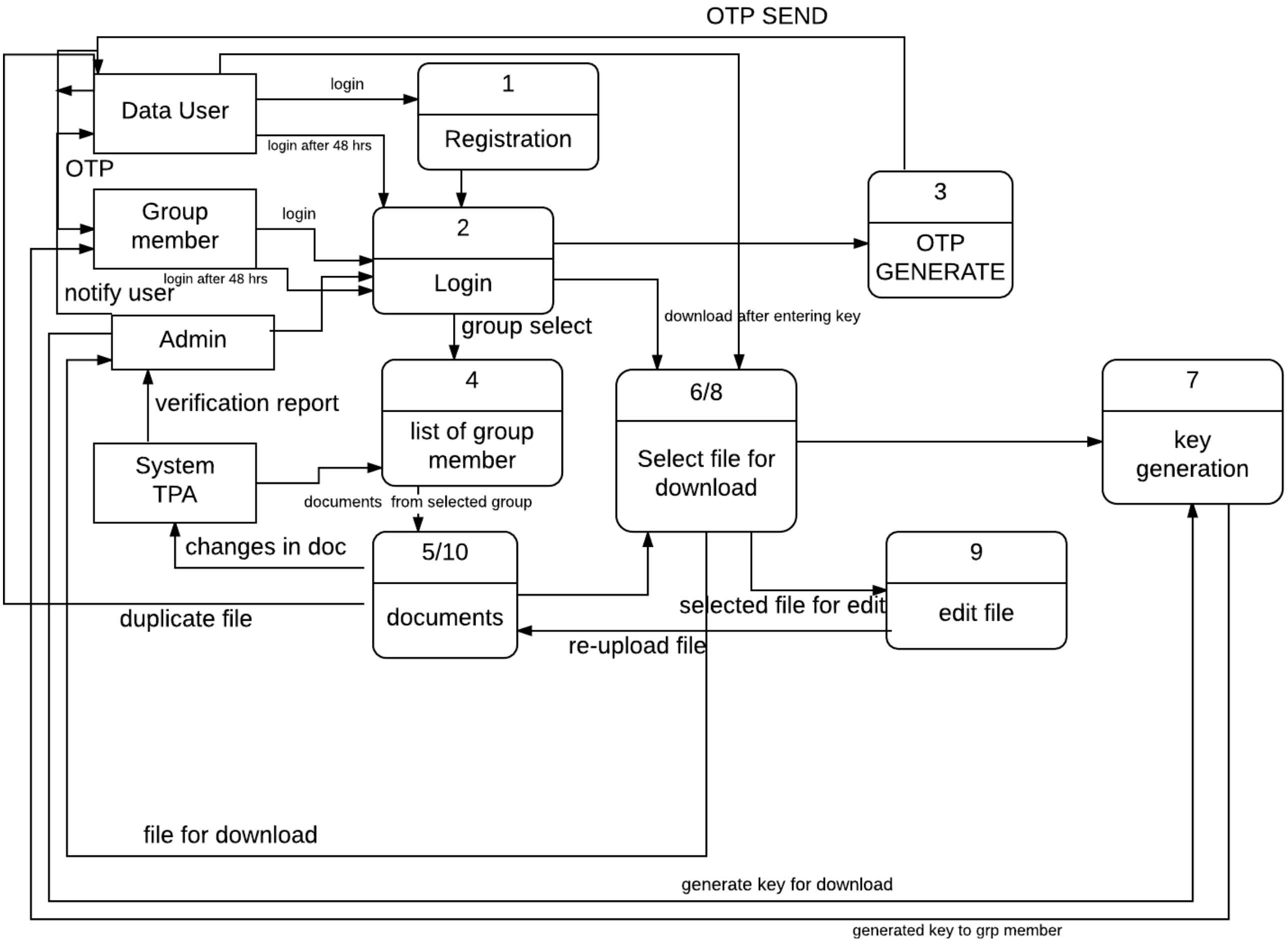

Figure 5: Detail data flow diagram

Class diagram

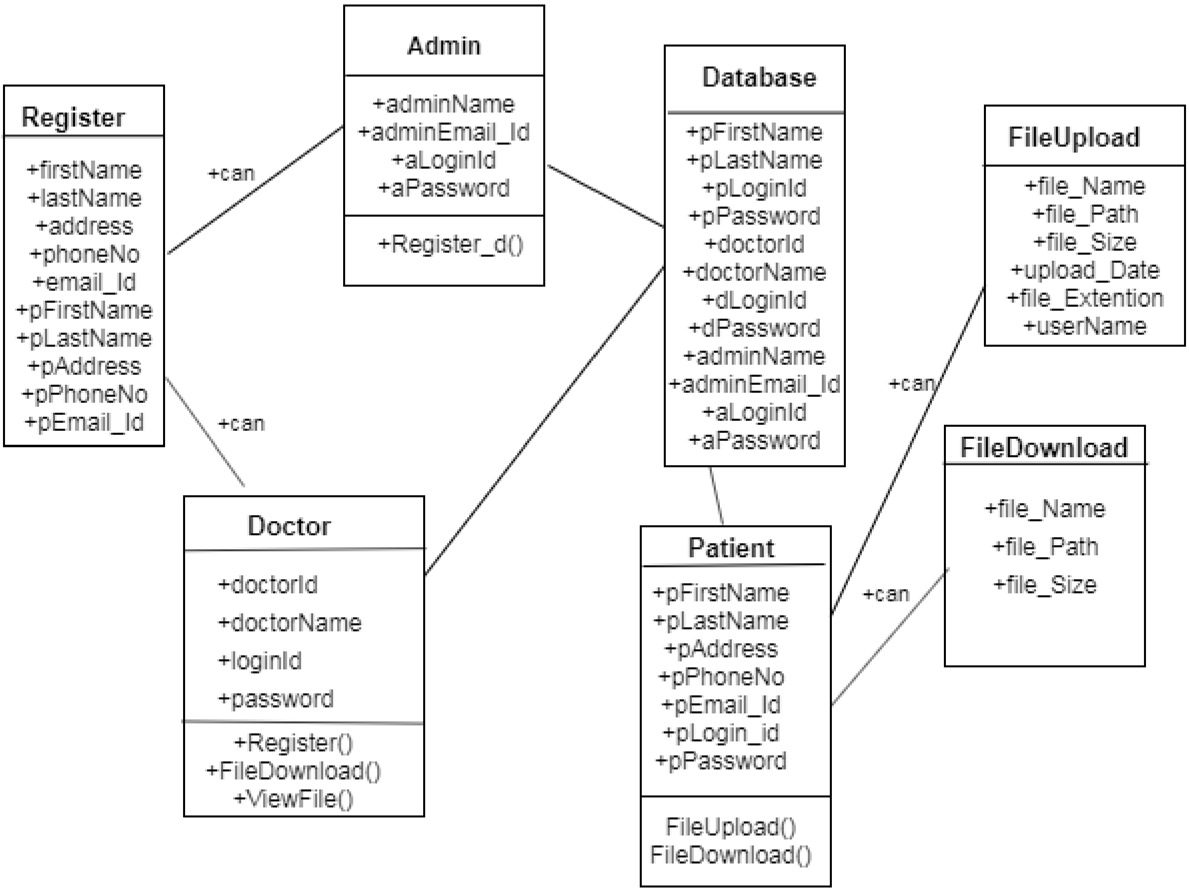

Figure 6: class diagram

Sequence diagram

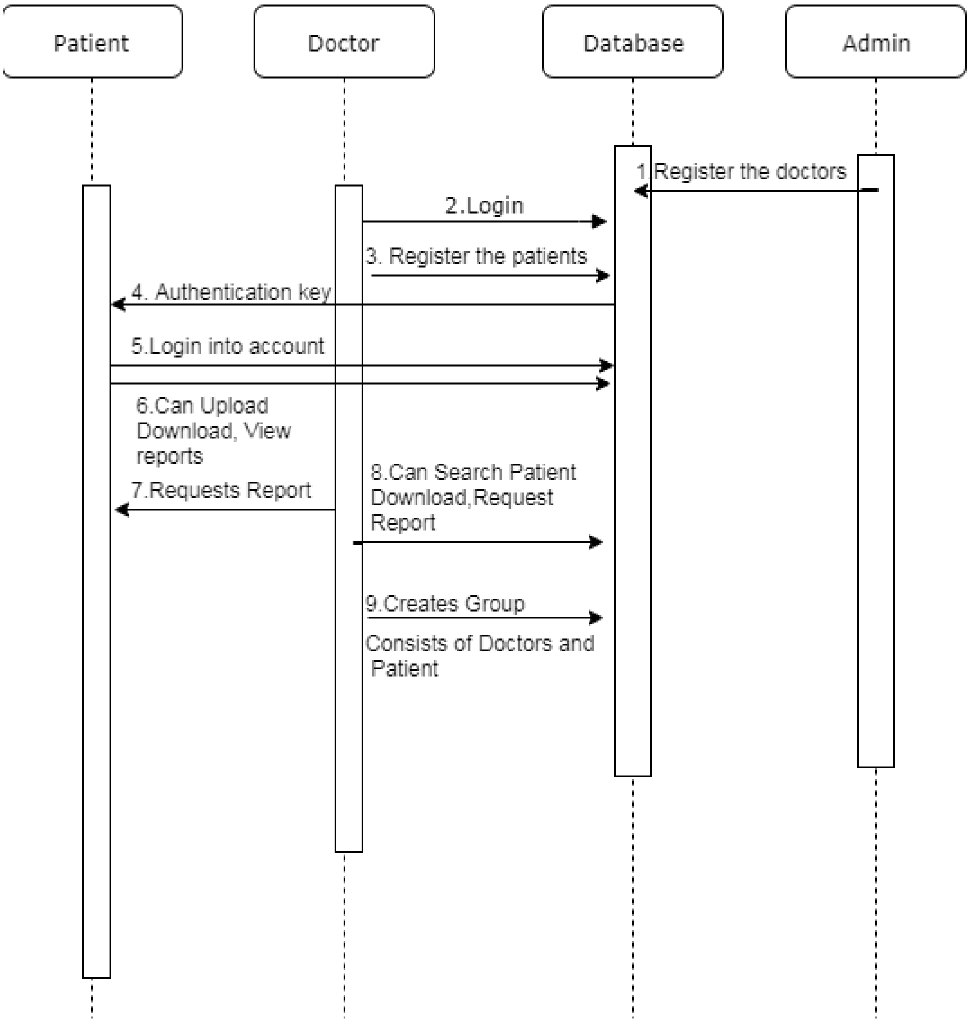

Figure 7: sequence diagram

Activity diagram

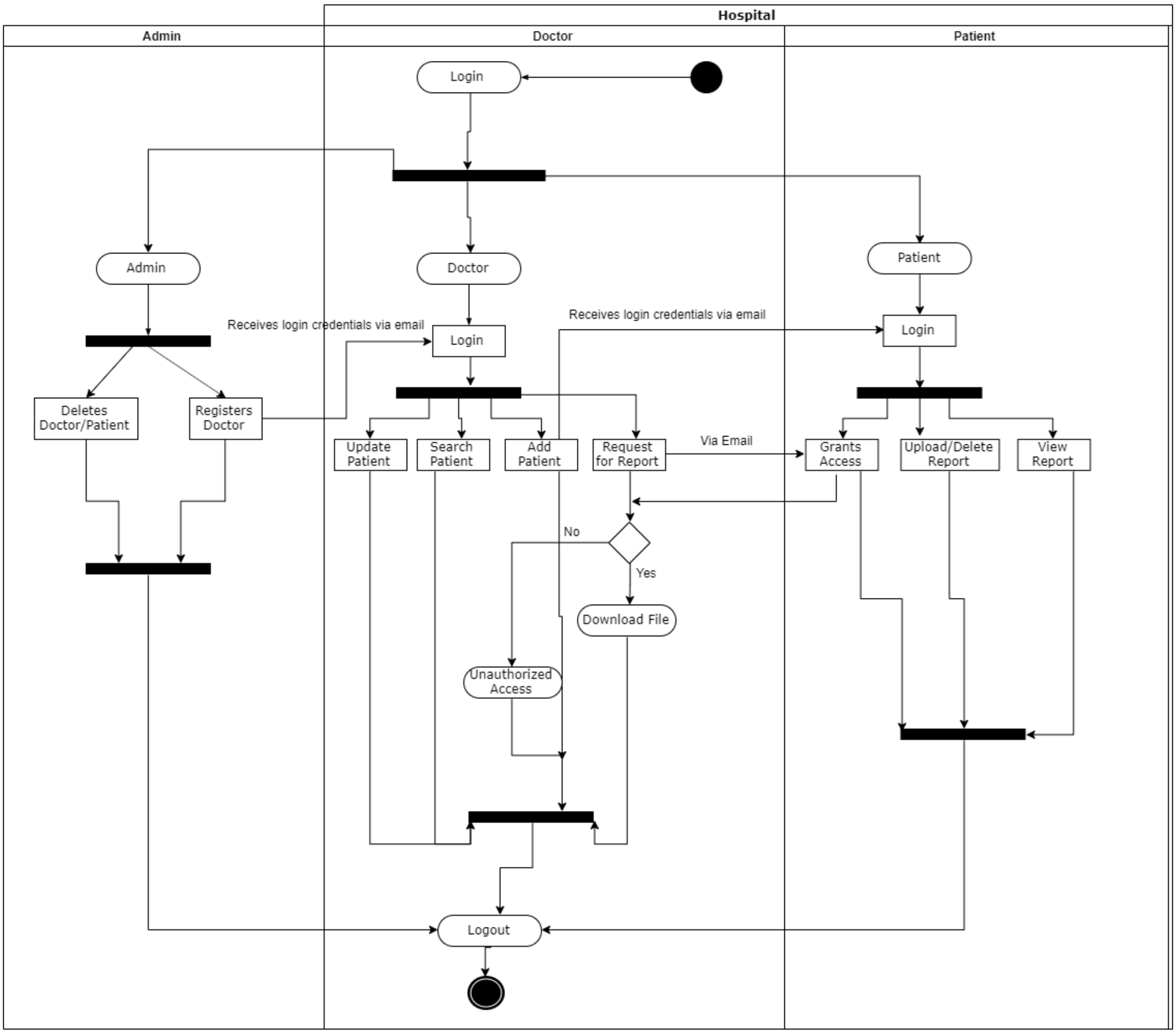

Figure 8: Activity diagram

Summary

The work presented in this report is related to Enhancing Data Security in Cloud using Blockchain

- Blockchain: A security mechanism used for storing data in a consecutive block like fashion with each previous block linked to the next using hash, used for securing data in the project.

- Cloud: In cloud large amount of data can be stored. Cloud is a service model in which data is maintained and made available to users over a network

References

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. Consulted, 2008.

[2] 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI) Amita Kashyap, G. Sravan Kumar, Sunita Jangir, Emmanuel S. Pilli, Preeti Mishra "IHIDS: Introspection-Based Hybrid Intrusion Detection System in Cloud Environment".

[3] Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., Kishigami, J. J. (2015). Blockchain contract: A complete consensus using blockchain. 2015 IEEE 4th Global Conference on Consumer Electronics (GCCEP).

[4] Zhe, D., Qinghong, W., Naizheng, S., Yuhan, Z. (2017). Study on Data Security Pol- icy Based on Cloud Storage. 2017 IEEE 3rd International Conference on Big Data Security on Cloud (Bigdata Security), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS).

[5] Bharadwaj, D. R., Bhattacharya, A., Chakkaravarthy, M. (2018). Cloud Threat Defense – A Threat Protection and Security Compliance Solution. 2018 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM).