Department of Information Technology

A.P. Shah Institute of Technology

G.B.Road,Kasarvadavli, Thane(W), Mumbai-400615

UNIVERSITY OF MUMBAI

Academic Year 2019-2020

A Project Report on

Enhancing Data Security in Cloud using Blockchain

Submitted in partial fulfillment of the degree of

Bachelor of Engineering(Sem-8)

in

INFORMATION TECHNOLOGY

By

Dhananjay Yadav(17204015)

Aditi Shinde(16104022)

Akash Nair(16104051)

Under the Guidance of

Prof. Yamini Patil

Prof.Sneha Kanchan

1.Project Conception and Initiation

1.1 Abstract

- Blockchain is a mechanism invented to secure data in more advance method.
- Data exchanged between the patient and doctors need to be secured to gain patients trust.
- Blockchain store data into chunks that make it hard to decode, which will help provide extra layer of security.
- This data can be secured by using an blockchain mechanism at the backend of any hospital website to store the reports of the patients, and maintain an two-way authentication for doctors access to the reports.

1.2 Objectives

- To provide effective security to the data uploaded by patients.
- To maintain better integrity of data on cloud.
- To avoid fraudery of data by storing data into buckets in a distributed manner.
- To maintain two-step authentication for access of reports by doctors.

1.3 Literature Review

Paper title:- Bitcoin: A peer-to-peer electronic cash system.
Author:-Nakamoto S
Publication details:- https://bitcoin.org/bitcoin.pdf
Findings:- Revised the implementation of blockchain as a technology with a wide scope and found its use in the first cryptocurrency ever created i.e. Bitcoin with blockchain as a technology and SHA-256 as its hash function. First general use of blockchain to secure transactions.
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.

Literature Review

Paper title:-Blockchain contract: A complete consensus using blockchain.
Author:- Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., & Kishigami
Publication details:- 2015 IEEE 4th Global Conference on Consumer Electronics.
Findings:- Use of blockchain consensus in online or data contracts and making it more secure. Consensus mechanism allows every party in the contract to share their consent regarding the contract which provides a secure and satisfactory result.
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.

Literature Review

Paper title:- IHIDS:Introspection-Based Hybrid Intrusion Detection System in Cloud Environment”

Author:- Amita Kashyap, G. Sravan Kumar, Sunita Jangir, Emmanuel S. Pilli, Preeti Mishra

Publication details:- 2017 IEEE

Findings:- Use of Intrusion detection system in the hypervisor layer of the cloud which allows the cloud owner and admin to be notified when in the midst of intrusion by an unauthorized party.

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 notifies the infiltration, it doesn’t lock it. Hence, at times it would be too late before the user or admin is notified.

1.4 Problem Definition

- In current scenario lot of fraudery on data takes place in Healthcare sector due to lack of security of the data and more use of hard-copies of reports.
- Providing blockchain mechanism to data will not only reduce the use of hard-copies but also provide a base of security on the data stored on cloud servers thus providing secure means of data transmission.

1.5 Scope

- To provide an interface that’s easy to use for both the doctor as well as patients.
- Will provide security to any confidential data of patient in the reports.
- Storing data in buckets in an distributed manner makes the data lot more secure.
- Using the mechanism of interlinking of hashes as blockchain and storing it into buckets maintains the CIA properties of security on data.

1.6 Technology stack

- Operating System : Windows 07 And Above
- Cloud platform : Cloud Service.
- AES : Cryptographic algorithm for creating hash values of data.
- Navicat : For visualization of database contents.
- Eclipse Luna : Integrated Development Environment (IDE) for java programming.
- My SQL : For Database storage.
- JDK : For programming as it is object oriented, easy to write, compile, debug, platform-independent.

Technology stack

- Blockchain Mechanism : For providing 3 main components to the data-cryptography, distributed list structures and a decentralized storage system. Depending on these three which can be implemented through software, blockchain can be open source or proprietary. It’s one of the latest technological trends now in the industry and provides a highly secure environment when used as compared to other cryptography and encryption standards.

1.7 Benefits for environment & Society

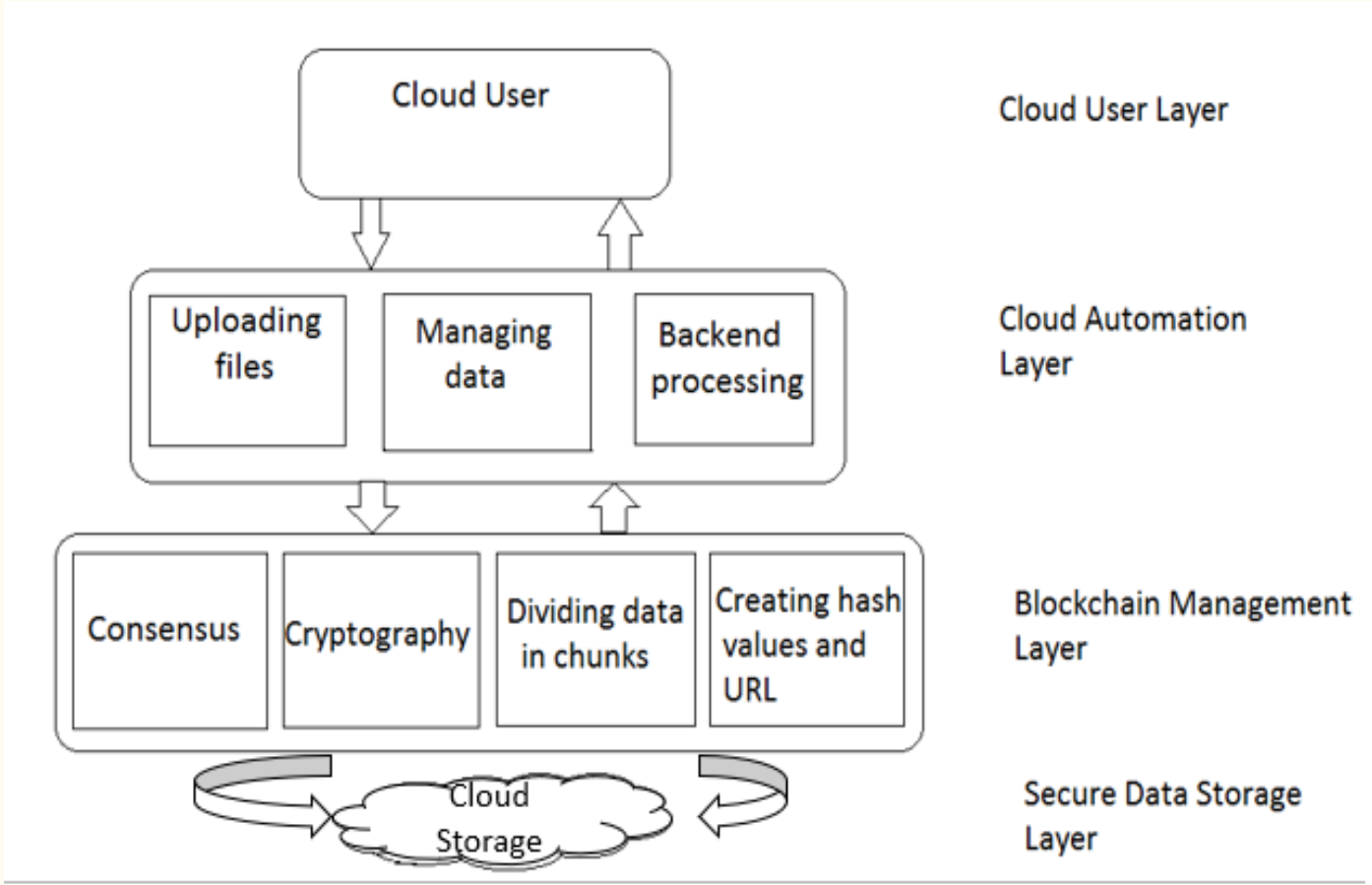
- Patients feel more secure about there data .
- Users are in control of all their information.
- Blockchain offers access security, scalability, and data privacy.
- Much advance security as blockchain needs high computational power to generate nonce value for each block.
- Keeping data more in softcopy will reduce the tension of disremembering and carrying files every time.

2. Project Design

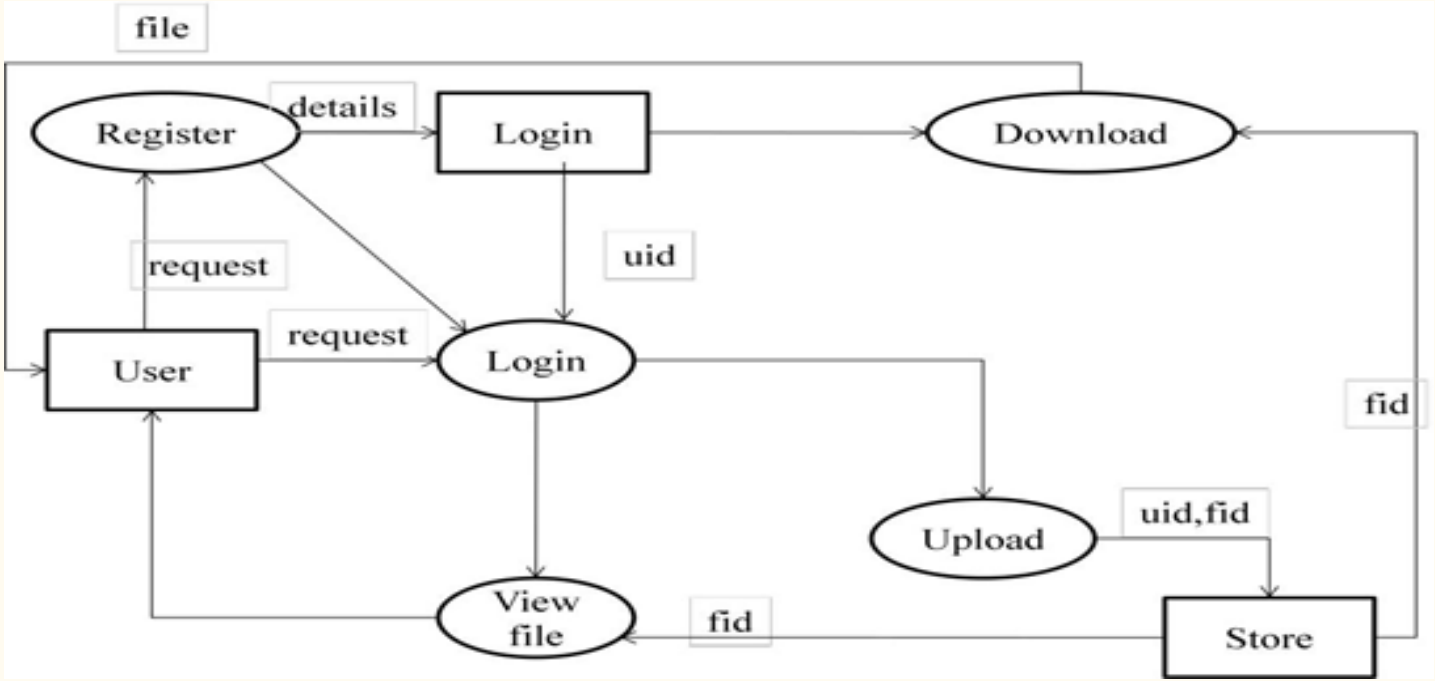
2.1 Proposed System

- UI for any hospital website.
- Logins for Admins, Doctors and Patients.
- Uploading reports and securing it through encryption and hash values in different buckets.
- Storage buckets to be maintained with the help of S3 provided by AWS.
- Maintaining an authentication from patients side for doctors to access the report.

2.1.1 Proposed System



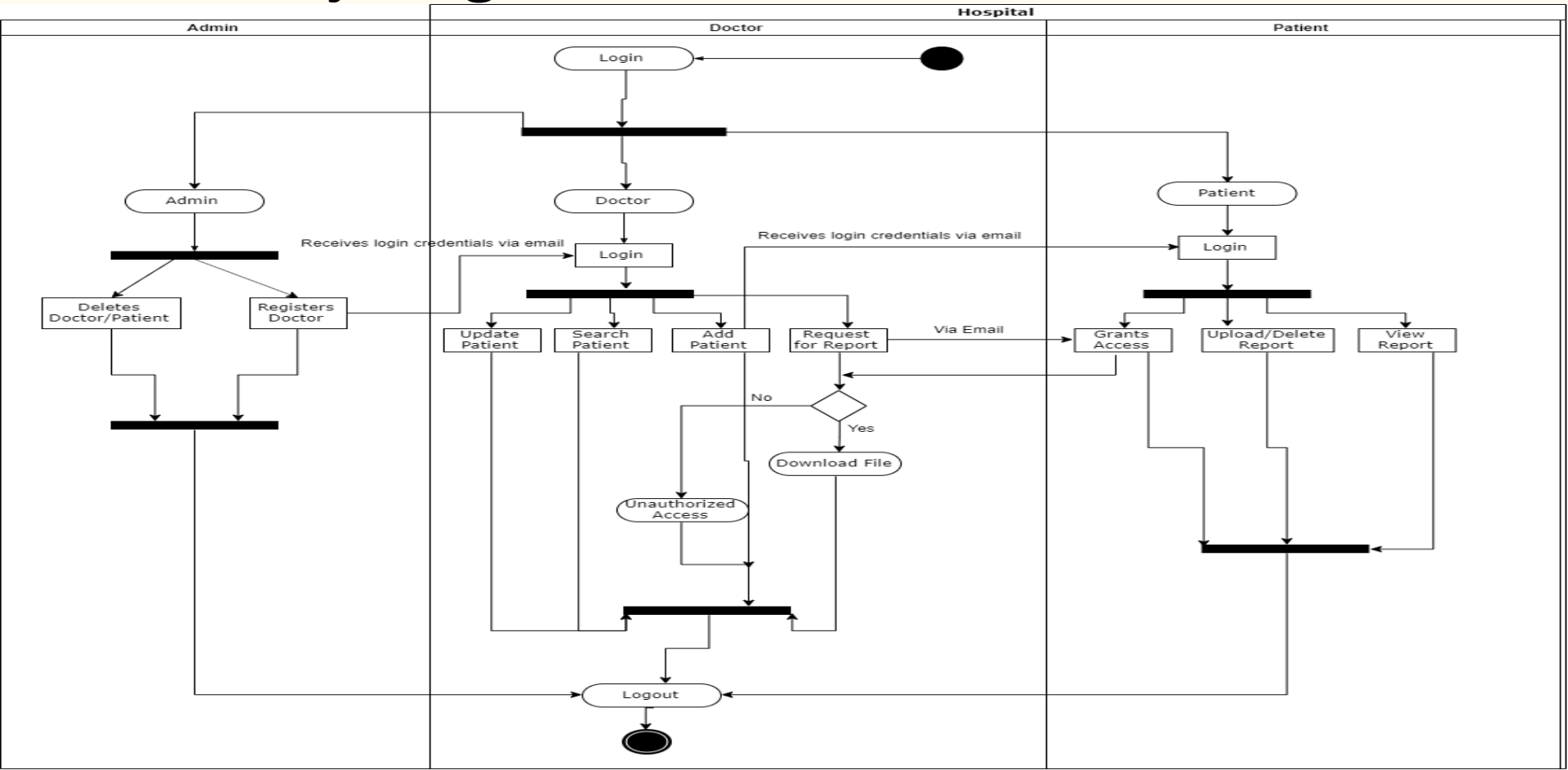
2.2 Design(Flow Of Modules)



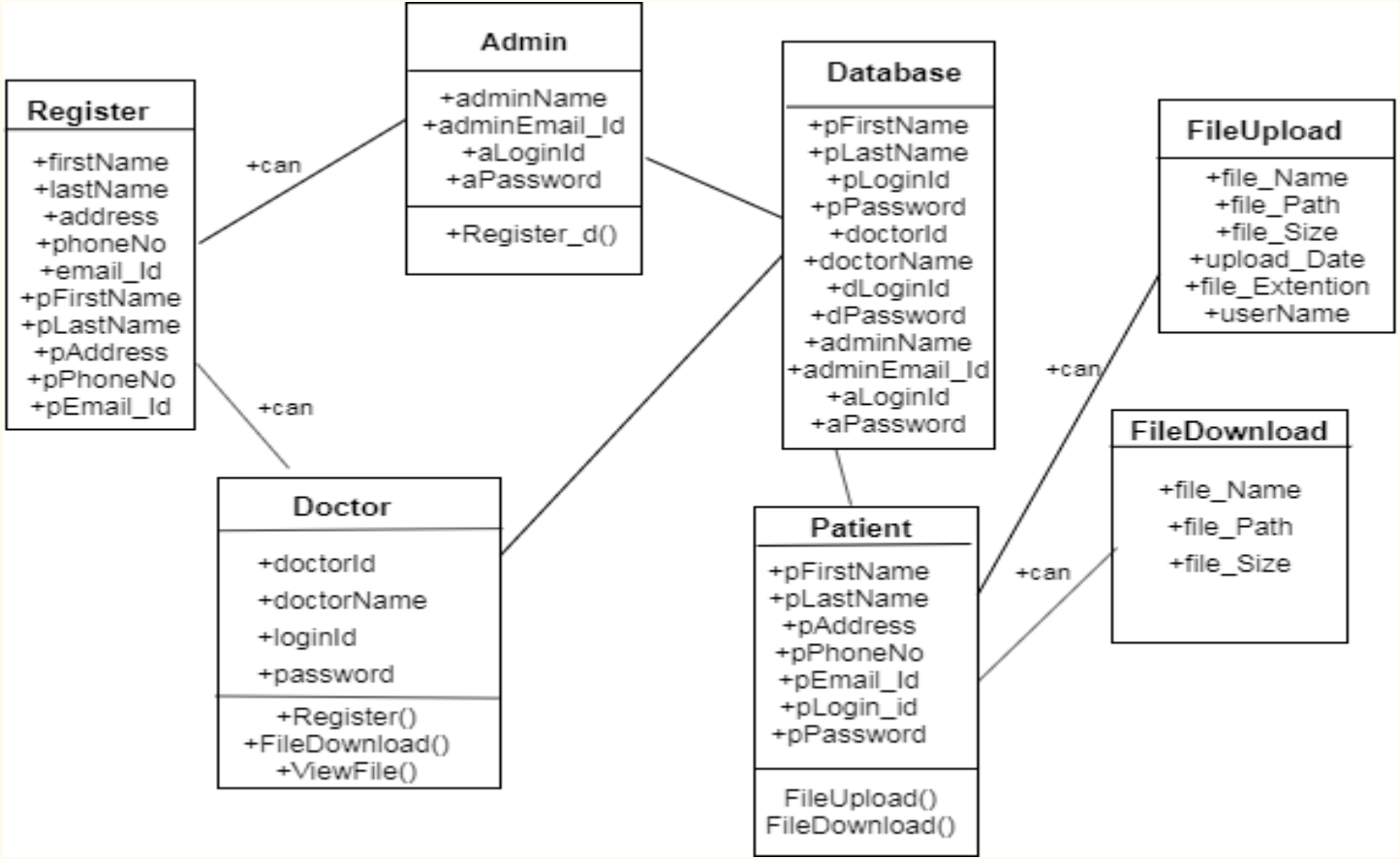
2.3 Description Of Use Case

- The Admin will add doctors and will have permissions to delete doctors and patients.
- Doctor will add new patients and can prescribe medicines, Doctors will need a key to download report that would be present with the patient.
- Patients can upload reports and grant access to view there reports.

2.4 Activity diagram



2.5 Class Diagram



2.6 Module-1

Web Interface:

- Admin side to manage the whole website for granting and revoking privileges to the other entities of website.
- Doctors Portal that would deal with dealing with patients like adding new patients, prescribing medicines, requesting to view report.
- Patients Portal that would be able to upload report, view there own report, grant access to authorized doctors for there report .

Module-2

Web Interface Backend

- Backend mainly concentrates on report uploading.
- Along with this it will consist of generating hash values and dividing it into chunks to stores it with the concept of blockchain.
- Some minor fields like storing user credentials for authentication, storing prescribed medicines.

Module-3

Blockchain & Hashing

- At first the data would be stored with the help of AES .
- After which the data would be divided into chunks and hash values would be generated
- These chunks with there hash values will be interconnected with the concept of blockchain.
- Storage will be done into S3 buckets.

2.7 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 Policy Based on Cloud Storage. 2017 IEEE 3rd International Conference on Big Data Security on Cloud (BigDataSecurity), 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).

3.Future Scope

Future Scope

- Can be implemented on any kind of data that is stored on the cloud.
- Can be used to provide security to any confidential data.
- Can be implemented in sectors like IT, Medical, Banking , etc.
- Healthcare sector can improve by including many different kind of reports
- Data collection can be maintained with better integrity if public blockchain is maintained to gather information from different countries during pandemics e.g:- Current situation of covid-19 is facing issues in collecting data to form pattern to overcome the pandemic.

Review from King Edward Memorial Hospital

- The project idea was discussed with one of the fellow doctor Dr. Vidhi Yadav (B.H.M.S , P.G.D.E.M.S)
- It was addressed as a good motive to secure patients report and make data available online.
- We were also addressed about how making two step authentication for accessing report makes it more reliable.

Thank You