

# **CSE6006–NoSQL Databases**

## **J Component - Project Report SECURED**

### **SHARING SENSITIVE DATA IN BANKING PLATFORM**

*By*

20MCS1006

A.JAFFLET TRINISHIA

M.Tech

**Review III Report**

*Submitted to*

**Dr.A.Bhuvaneswari,**  
Assistant Professor Senior,  
SCOPE, VIT, Chennai

**School of Computer Science and Engineering**

*March 2021*



**VIT<sup>®</sup>**

**Vellore Institute of Technology**

(Deemed to be University under section 3 of UGC Act, 1956)

## Abstract:

Clients store tremendous measures of touchy information on a major information stage. Sharing delicate information will assist undertakings with decreasing the expense of giving clients customized benefits and offer some incentive added information administrations. In any case, secure information sharing is tricky. This paper proposes a system for secure touchy information sharing on a major information stage, including secure information conveyance, stockpiling, utilization, and obliteration on a semi-believed huge information sharing stage. We present an intermediary re-encryption calculation dependent on heterogeneous ciphertext change and a client interaction assurance technique dependent on a virtual machine screen, which offers help for the acknowledgment of framework capacities. The system ensures the security of clients' delicate information adequately and shares these information securely. Simultaneously, information proprietors hold full oversight of their own information in a sound climate for present day Internet data security.

## Introduction:

With the fast advancement of data digitization, massive measures of organized, semi-organized, and unstructured information are produced rapidly. By gathering, arranging, dissecting, and mining these information, an endeavor can acquire a lot of individual clients' touchy information. These information not just fulfill the needs of the actual endeavor, yet additionally offer types of assistance to different organizations if the information are put away on a bigdata stage. Conventional distributed storage only stores plain content or encoded information inactively. Such information can be considered as "dead", since they are not engaged with computation. Be that as it may, a major information stage permits the trading of information (counting touchy information). It gives mass information stockpiling and computational administrations. Calculation administrations allude fundamentally to activities, (for example, scrambling information, change, or capacity encryption) on information utilized by members, which can stimulate "dead" information. An illustration of suchan application is appeared in

At the point when Alice presents an inquiry (active apparel), the Search Engine Service Provider (SESP) first searches for Alice's inclination on the huge information stage. In the event that the large information stage has gathered and shared the client's very own inclination data, "badminton", at that point the internet searcher returns customized results(sportswear + badminton) to Alice. At the point when Alice sees

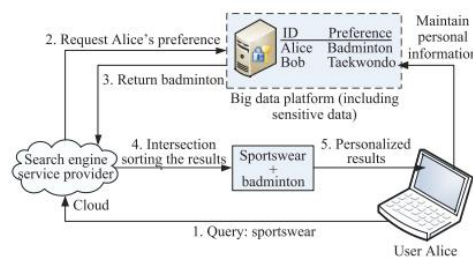


Fig. 1 Application of sensitive data (user's preferences).

her favorite badminton athletic apparel, she encounters pleasant buy. Thusly, this prompts a wining circumstance. Be that as it may, while information sharing expands undertaking

resources, Internet instability and the capability of delicate information spillage likewise make security issues for touchy information sharing.

Secure delicate information sharing includes four essential wellbeing factors. In the first place, there are security issues when sensitive information are communicated from an information proprietor's nearby worker to a major information stage. Second, there can be touchy information processing and capacity security issues on the huge information stage. Third, there are secure delicate information use issues on the cloud stage. Fourth, there are issues including secure information annihilation. Some examination establishments and researchers at home and abroad have made positive commitments to investigation and exploration pointed toward taking care of these security issues. Existing innovations have part of the way settled information sharing and security insurance issues from different points of view, however they have not considered the whole interaction in the full information security life cycle. Notwithstanding, a major information stage is a finished framework with multi-stakeholder inclusion, and hence can't endure any security penetrate bringing about delicate information misfortune. , we investigate security issues including the whole touchy information sharing life cycle and portray a system model made to guarantee secure delicate information sharing on a major information stage, to ensure secure capacity on the enormous information stage utilizing " Proxy Re-Encryption (PRE)" innovation, and to guarantee secure utilization of delicate information sharing utilizing a private space measure dependent on a "Virtual Machine Monitor (VMM)." Then, a security module and an information implosion system help to mitigate client concern with respect to touchy individual data spillage.

### **Project Objectives :**

1. Input Design is the way toward changing over a client situated depiction of the contribution to a PC based framework. This plan is essential to keep away from blunders in the information input interaction and show the right heading to the administration for getting right data from the electronic situation.

2. It is accomplished by making easy to understand evaluates for the information section to deal with huge volume of information. The objective of planning input is to make information section simpler and to be liberated from mistakes. The information section screen is planned so that all the information controls can be performed. It additionally gives record seeing offices.

3. When the information is entered it will check for its legitimacy. Information can be entered with the assistance of screens. Suitable messages are given as when required with the goal that the client

won't be in maize of moment. In this way the goal of info configuration is to make an information format that is not difficult to follow

### **Problem Statement**

Existing technologies have partially resolved data sharing and privacy protection issues from various perspectives, but they have not considered the entire process in the full data security life cycle. However, a big data platform is a complete system with multistakeholder involvement, and thus cannot tolerate any security breach resulting in sensitive data loss.

Existing technologies have partially resolved data sharing and privacy protection issues from various perspectives, but they have not considered the entire process in the full data security life cycle.

#### **a. Research challenges**

The Primary challenges in the plan of the project :

1. Provide clients a prepared-to-utilize, expressive visual displaying Language with the goal that they can create and trade significant models.
2. Provide extendibility and specialization instruments to expand the center ideas.
3. Be autonomous of specific programming dialects and advancement measure.
4. Provide a proper reason for understanding the demonstrating language.
5. Support more significant level advancement ideas like coordinated efforts, systems, examples and segments.
6. Integrate accepted procedures.

#### **Towards Encrypting Industrial Data on Public Distributed Networks**

**Author:** [J. D. Preece](#); [J. M. Easton](#)

This paper addresses the problem of uploading large quantities of sensitive industrial data to a public distributed network by proposing a new framework. The framework combines the existing technologies of the distributed web and distributed ledger to provide a mechanism of encrypting data and choosing whom to share the data with. The framework is designed to work with existing platforms; the Inter Planetary File System (IPFS) and the Ethereum block chain platforms are used as examples within this paper, though it is stated that similar platforms are capable of providing the requirements for the framework to operate. The framework uses the concept of the Diffie-Hellman Key Exchange (DHKE), and is implemented in three different mechanisms of the DHKE: one-step Elliptical-Curve Diffie-Hellman Key Exchange (ECDH); two-step ECDH; and Super singular Isogenies Diffie-Hellman Key Exchange (SIDH). The paper discusses the security of each along with individual advantages and disadvantages, and concludes that the SIDH is the most appropriate implementation for future use due to it being post-quantum secure.

#### **Trust-based Scheduling Framework for Big Data Processing with MapReduce**

**Author:** Dat Thanh Dang; Doan Hoang; Diep Nguyen

Security and privacy have become a great concern in cloud computing platforms in which users risk the leakage of their private data. The leakage can happen while the data is at rest (in storage), in processing, or on moving within a cloud or between different cloud infrastructures, e.g., from private to public clouds. This paper focuses on protecting data "in processing". For big data applications, the Map Reduce framework has been proven as an efficient solution and has been widely deployed, e.g., in healthcare and business data analysis. In this article, we propose a trust-based framework for Map Reduce in big data processing tasks. Specifically, we first quantify and propose to assign the sensitive values for data and trust values for map and reduce slots. We then compute the trust value of each resource employed in the big data processing tasks. Depending on the data's sensitivity level of a task, the task requires a given level of trust (i.e., higher sensitive data requires servers/slots with higher trust level). The Map Reduce scheduling problem is then formulated as the maximum weighted matching problem of a bipartite graph that aims to maximize the total trust value over all possible assignments subject to various trust requirement of different tasks. The problem is known to be NP-hard. To tackle it, we observe that within a computing node (VM), slots share the same trust value granted from the secured transformation phase. This helps reduce the number of slot nodes of a weight bipartite graph. Leveraging this fact, we propose an efficient heuristic algorithm that achieves 94.7% of the optimal solution obtained via exhaustive search. Extensive simulations show that the trust-based scheduling scheme provides much higher protection for data sensitivity while ensuring good performance for big data applications

**Post study of Block chain in smart health environment Author:**

[Mansukhdeep Kaur](#); [Mohsin Murtaza](#); [Mostafa Habbal](#)

Block chain technology is being popular day by day and also serving in many applications and areas such as Internet of Things, Cloud Computing, Big data, Healthcare and many more because of its security strengths and benefits. It has been proven that block chain applications are being utilized in healthcare to deliver secure data and to manage the medical data safely. Moreover, block chain is transforming the traditional medical practices in effective ways such as diagnosing the problems effectively and treating through secure information sharing. There is no doubt to say that in future, block chain will be performing in personalized, valid and secure healthcare by combining the medical information of patient and providing in a secure and updated setup. In this research paper, securities of healthcare applications and traditional and recent security developments are discussed. Due to Covid-19, it has become challenging for healthcare officials and government to protect and record individuals sensitive data safely. Also, spread of misleading information has been also increased during the pandemic and inability of existing platform for information validation leads to public panic. Implementation of block chain-based tracking systems is essential for accurate and valid information sharing among people and Government. This paper focus on information security issues raised by Covid-19 pandemic as well as implementation of block chain-based platform in healthcare to record and protect covid-19 related information and contact tracing.

**A Secure and Lightweight Data Access Control Scheme for Mobile**

## **Cloud Computing**

**Author:** [Yu Jin](#); [Chuan Tian](#); [Heng He](#); [Fan Wang](#)

By moving data storage and processing from lightweight mobile devices to powerful and centralized computing platforms located in clouds, Mobile

Cloud Computing (MCC) can greatly enhance the capability of mobile devices. However, when data owners outsource sensitive data to mobile cloud for sharing, the data is outside of their trusted domain and can potentially be granted to untrusted parties which include the service providers. Data security and flexible access control have become the most pressing demands for MCC. To address this issue, we design a secure and lightweight data access control scheme based on Cipher text-Policy Attribute-based Encryption (CP-ABE) algorithm, which can protect the confidentiality of outsourced data and provide fine-grained data access control in MCC. The scheme can obviously improve the overall system performance by greatly reducing the computation overheads in encryption and decryption operations, provide flexible and expressive data access control policy, and meanwhile enable data owners to securely outsource most of the computation overheads at mobile devices to cloud servers. The security and performance evaluation show that our scheme is secure, highly efficient and well suited for lightweight mobile devices.

## **Secure sensitive data sharing on a big data platform Author:**

Xinhua Dong; Ruixuan Li; Heng He; Wanwan Zhou

Users store vast amounts of sensitive data on a big data platform. Sharing sensitive data will help enterprises reduce the cost of providing users with personalized services and provide value-added data services. However, secure data sharing is problematic. This paper proposes a framework for secure sensitive data sharing on a big data platform, including secure data delivery, storage, usage, and destruction on a semi-trusted big data sharing platform. We present a proxy re-encryption algorithm based on heterogeneous cipher text transformation and a user process protection method based on a virtual machine monitor, which provides support for the realization of system functions. The framework protects the security of users' sensitive data effectively and shares these data safely. At the same time, data owners retain complete control of their own data in a sound environment for modern Internet information security.

## **Secure Proxy-Reencryption-Based Inter-Network Key Exchange**

**Author:** Lloyd Greenwald; Kurt Rohloff

In this paper we present a novel approach to distribute session keys securely across administrative boundaries where participants may be unable to interact directly. The basis of our approach is the use of Proxy Re-Encryption (PRE) to encrypt session keys (e.g., AES keys), publish the session keys to a proxy server, and then distribute the session keys to session participants who re-encrypt, decrypt and access the session keys.

Our approach, Secure Proxy-Re-encryption-based Inter-network Key Exchange (SPIKE), applies to several real world use cases, including coalition data sharing, sensor network data sharing and large-scale video distribution. SPIKE enables these use cases without requiring coordination between publishers and subscribers. We address an honest-but-curious adversary model where any data sent over a network link or stored at a proxy can be leaked. Our design of SPIKE is independent of the specific PRE scheme used. For implementation and experimentation purposes we implement and use, PALISADE, a general post-quantum lattice-based encryption library that provides a unidirectional PRE scheme with collusion resistance, supports multi-hop re-encryption, and admits more general homomorphic encryption properties than other schemes. We present our design and implementation in experimental settings to evaluate real world performance. We discuss generalization of our approach to increase scalability and address broader security concerns.

### **Performance Analysis of the Symmetric Proxy Re-encryption Scheme**

**Author:** [Rizky Putri Meiliasari](#); [AmrilSyalim](#); [Setiadi Yazid](#)

The use of cloud system's storage service has been increasing in recent years. A way to secure the stored data is to use cryptographic techniques. One of the techniques that can be used when sharing data accesses with other users, is proxy re-encryption, which means converting data from its unreadable form (cipher text) corresponding to one key into another cipher text of a different key. Many proxy re- encryption schemes often only use asymmetric key cryptography, and not symmetric key. In this paper we analyze the performance of a symmetric proxy re-encryption scheme's implementation. In measuring the performance of the re-encryption function, the authors compare the running time of the program with that of AES CBC's re-encryption's running time, to compare a naïve re-encryption with the selected schemes. We also propose some improvement to the implementation of the proxy re-encryption algorithm.

### **A New Dynamic Conditional Proxy Broadcast Re-Encryption Scheme for Cloud Storage and Sharing**

**Author:** [Zhanwen Chen](#); [Jiageng Chen](#); [Weizhi Meng](#)

Security of cloud storage and sharing is concerned for years since a semi-trusted party, Cloud Server Provider (CSP), has access to user data on cloud server that may leak users' private data without constraint. Intuitively, an efficient solution of protecting cloud data is to encrypt it before uploading to the cloud server. However, a new requirement, data sharing, makes it difficult to manage secret keys among data owners and target users. Therefore conditional proxy broadcast re- encryption technology (CPBRE) is proposed in recent years to provide data encryption and sharing approaches for cloud environment. It enables a data owner to upload encrypted data to the cloud server and a third party proxy can re-encrypted cloud data under certain condition to a new cipher text so that target users can decrypt re- encrypted data using their own private key. But few CPBRE schemes are applicable for a dynamic cloud environment. In this paper, we propose a new dynamic conditional proxy broadcast re-encryption scheme that can be dynamic in system user setting and target user group. The initialization phase does not require a fixed system user setup so that users can join or leave the system in any time. And data owner can



dynamically change the group of user he wants to share data with. We also provide security analysis which proves our scheme to be secure against CSP, and performance analysis shows that our scheme exceeds other schemes in terms of functionality and resource cost.

### **CCA Secure Proxy Re-Encryption Scheme for Secure Sharing of Files through Cloud Storage**

**Author:** Bharati Mishra; Debsish Jena

Cloud Storage Service(CSS) provides unbounded, robust file storage capability and facilitates for pay-per-use and collaborative work to end users. But due to security issues like lack of confidentiality, malicious insiders, it has not gained wide spread acceptance to store sensitive information. Researchers have proposed proxy re- encryption schemes for secure data sharing through cloud. Due to advancement of computing technologies and advent of quantum computing algorithms, security of existing schemes can be compromised within seconds. Hence there is a need for designing security schemes which can be quantum computing resistant. In this paper, a secure file sharing scheme through cloud storage using proxy re-encryption technique has been proposed. The proposed scheme is proven to be chosen cipher text secure(CCA) under hardness of ring-LWE, Search problem using random oracle model. The proposed scheme outperforms the existing CCA secure schemes in-terms of re-encryption time and decryption time for encrypted files which results in an efficient file sharing scheme through cloud storage.

### **Improved Proxy Re-Encryption With Delegatable Verifiability**

Author: [Yu Zhan](#); [Baocang Wang](#); [Zheng Wang](#); [Tao Pei](#); [Yuan Chen](#)

Proxy re-encryption cryptosystem enables proxy to re-encrypt the cipher text and protects the privacy of the corresponding plaintext. Hence, this type of cryptosystem has found tremendous applications in data sharing in cloud computing, email forwarding, securing file systems, and so on. In practice, proxy re-encryption has to support verification of cipher text to reduce the users' computational burden. The cipher text verification can be achieved through a public, private, or delegate able manner. Delegatable verification is more generic in that it can be easily converted into the other two verification methods. However, almost all existing schemes with delegate able verifiability only achieve replay able chosen cipher text security. Hence, in this paper we propose a more secure proxy re-encryption scheme with delegatable verifiability. Specifically, we utilize a short signature scheme to prevent an attacker from forging a valid cipher text, and prevent an attacker from forging a signature. As a result, our scheme is secure against chosen cipher text attacks under the standard model.

#### **2. Data Set Description:**

Here we are not using dataset which is there is no pre defined dataset We are creating data set Form with 63 data per user we can also include as many datas as we want these datas will be stored into the dataser that we are creating

Data set consist of four parts namely

1. General information like

1. Name
2. DOB
3. Gender

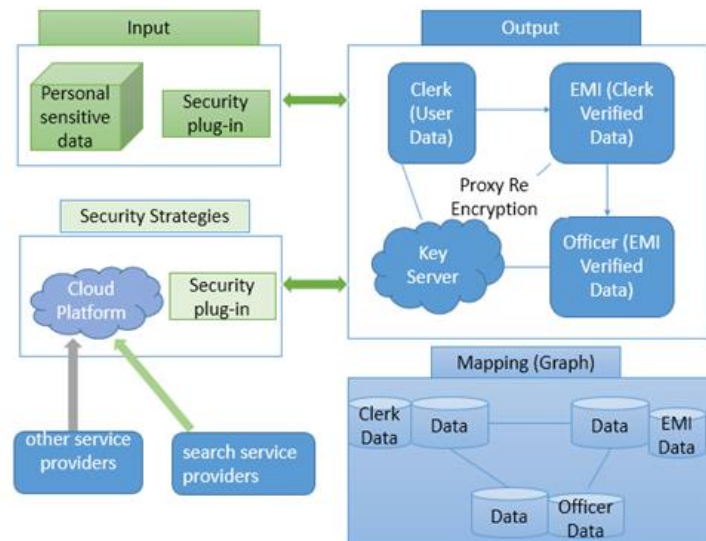


4. mail id
5. phone number
6. address
2. Previous loan details like
  - emi and other information of the user
3. other Information like
  - Information about the property
  - vehicle of the customer
  - Information about the job
4. Loan amount require
  - Purpose
  - Amount
  - Percentage of interest

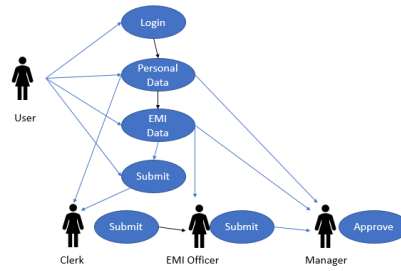
Description of the data source

### 3. Methodology and Algorithm used:

#### a. System Architecture diagram



#### b. Flowchart



#### c. Algorithm design

We proposed an efficient structure of secure sharing of touchy information on large information stage, which guarantees secure accommodation and capacity of delicate information dependent on the heterogeneous intermediary re-encryption calculation, and ensures secure utilization of clear content in the cloud stage by the private space of client measure dependent on the VMM. The proposed system well ensures the security of clients' delicate information. Simultaneously the information proprietors have the unlimited oversight of their own information, which is an achievable answer for balance the advantages of included gatherings under the semi-confided in conditions. Later on, we will upgrade the heterogeneous intermediary re-encryption calculation, and further improve the effectiveness of encryption. Likewise, diminishing the overhead of the communication among included gatherings is additionally a significant future work

### 4. Experimental setup

#### Hardware Requirements:

System- Pentium	—	IV 2.4 GHz
Speed	-	1.1 Ghz
RAM	-	256MB(min)
Hard Disk	-	40 GB
Key Board	-	Standard Windows Keyboard
Mouse	-	Logitech
Monitor	-	15 VGA Color.

#### Software Requirements:

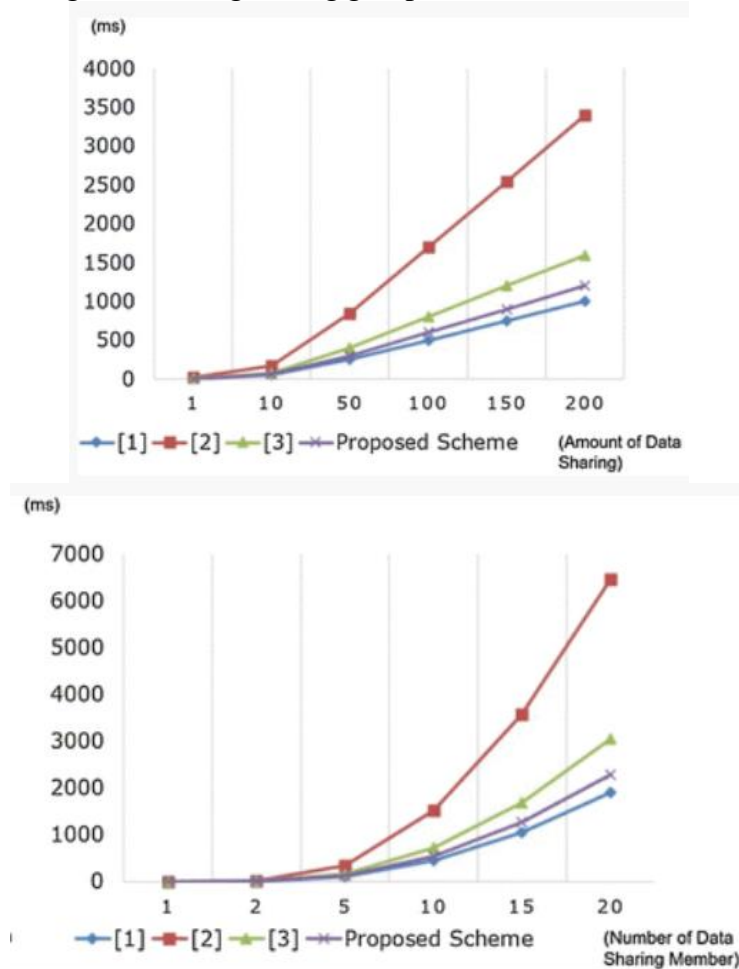
- ❖ Operating System : Windows/XP/7.
- ❖ Application Server : Tomcat 5.0/6.0
- ❖ Front End : HTML, Java, Jsp
- ❖ Scripts: JavaScript.
- ❖ Server side Script : Java Server Pages.
- ❖ Database : MongoDB
- ❖ Database Connectivity : Robomongo-0.8.5-i386.

### 5. Results and Discussion

#### A. Discussion of performance metrics

The proposed structure can give successful estimation during data

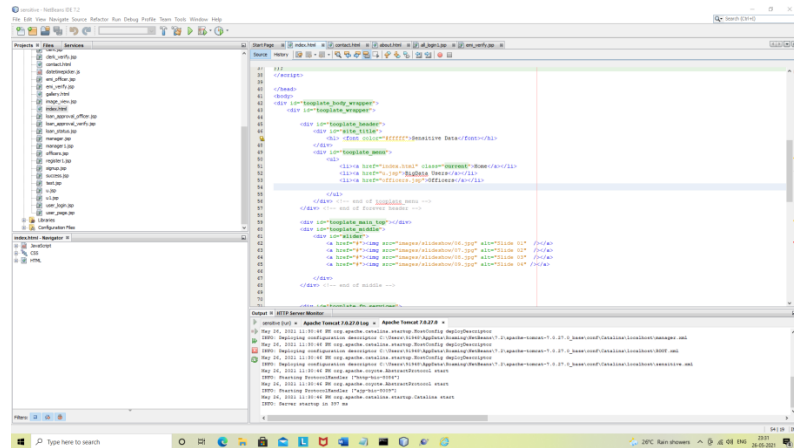
sharing, by performing lightweight mixing computation over the dispersed stockpiling laborer, which can't be trusted, through re-encryption. Besides, the proposed technique is more successful than existing systems in that it can move the encryption key by re-scrambling only the key, rather than re-encoding the genuine data or moving all the data. The Data, wherein the computation load during data sharing is pondered, the proposed methodology is more capable than existing methodologies to the extent the addition in data sharing defer time during estimation. Additionally, the data estimation load according to the amount of shared people is shown be especially capable during data sharing among groups.



### B.Comparison Graph

In existing System the information misfortune is high on the diverse classification like individual subtleties, Phone Number, Money and Charges on bank advance cycle. The level of misfortune on this class is plotted as a chart with the correlation on existing framework and the proposed approach. In proposed framework the misfortune are less contrasting with existing framework. The worth of misfortune is exceptionally low in proposed framework. More often than not their objective is telephone number of the client to promote something and make them to purchase that. In proposed technique utilizing intermediary re encryption the information is more gotten and it is more muddled to take the information. The proficiency of the proposed technique is 99.9%.





- This will open a local host page with the login page for both the workers and the users



- This is the user login page enter the user name and password and login

The screenshot shows the "Big Data User Authentication Page". It has a header with the title "Big Data User Authentication Page". Below the header is a blue bar with the text "Fill The Authentication Page". The main content area is titled "What type of Big Data User are you?" and includes a question: "Are you taking control of your data, or is Big Data just the latest Buzzword? Answer these 5 questions to find out what type of Big Data user you are and what your next steps should be to take advantage of Big Data's true potential." Below this, there are three cartoon characters representing different user types: "Big Data Super User", "Big Data Fast Follower", and "Big Data Rookie". To the right of the text is a login form with two input fields: "Authenticator Name" (containing "trishia") and "Password" (containing "\*\*\*\*\*"). Below the fields is a "Submit Query" button. At the bottom right, there is a link for "New User SignUp". The footer of the page says "Powered by SnapApp™".

- newly applying user should fill the below mentioned details that are related to the loan process

Please Tell Us more about Yourself

Permanent Address

Telephone(Permanent Residence)

People staying at permanent Residence
☐ Parents
☐ Siblings
☐ Spouse
☐ Others

Preferred Mailing Address
☐ Residence
☐ Office

Type of Vehicle you currently own
☐ Car
☐ Two-Wheeler

Ownership
☐ Self
☐ Financed
☐ Company Provided

Please Tell Us About your Occupation and Income Details

1.If salaried, you work for :

☐ Public Sector
☐ State Government
☐ Central Government
☐ MNC
☐ Public Limited company
☐ Private Limited company
☐ Partnership

2.If not salaried, you are :

☐ D-Individual Director
☐ E-Individual Self Employed
☐ R-Individual Partner
☐ U-Sole Proprietorship
☐ F-Partnership Firm
☐ C-Private Limited company

3. If self-employed, your nature of business:

☐ Trading
☐ Manufacturing
☐ consultancy
☐ Real-Estate
☐ Transporter
☐ Contractor

Details of Existing Loan and Liabilities

Loan No
Institution Name

Type Of Loan
Loan Amount

EMI Amount
Current Outstanding

Balance Tenor

- at last the values has to be acknowledged by the user and the values will be submitted the values submitted moves to the clerk for verification

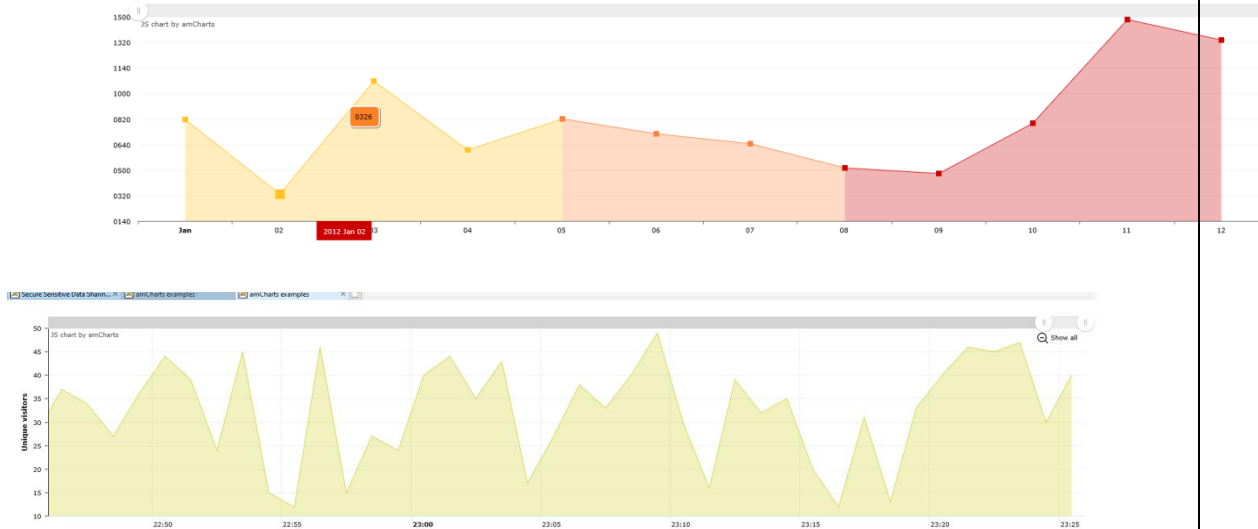
Submit Query

Declaration Form

I/We hereby authorize Mr./Ms. \_\_\_\_\_, Officer of Citibank N.A. India to assist me in completing my application form and related documents, prior to my signing the Application Form. It is my responsibility to read, understand and satisfy myself that the contents mentioned on the Application form are filled as per my instructions as to the correctness and completeness in all respects, prior to signing and it is binding on me/us. I/We understand that this loan is at sole discretion of the Bank. I/We confirm that I/we have by our own hand filled this application form and all details as given above to the Bank are true and correct and no material information had been suppressed/withheld. I/We confirm that the funds shall be used for the stated purpose only and shall not be used for speculative and/or capital market use and/or investments into Citi wealth management products and/or business and use purpose or prohibited/ antisocial purposes and/or purchase of gold/gold bullions/gold coins/gold jewelry/gold exchange traded funds/gold mutual funds. In the event that the loan funds have been used for purposes as prohibited above, the Bank shall be entitled to do all acts and things that the Bank deem necessary to comply with its policies, including but not limited to liquidating my/our holdings of investments at that time. I/We agree to bear all costs and expenses the Bank incur as a result thereof. I/we further certify that I/we am/are citizen(s) of India I/we undertake to inform the Bank of any change in residential status.

Browse...

- the bellow mentioned graph tells about the status of the bank and the current date time and share rate (it is just a prototype model ) and the 2<sup>nd</sup> graph tells when the bank is



- The details of the users are now moved to the clerk for verification the loan amount applied by the users will not be visible to clerk but the encrypted form will be visible after verifying the details it will be forwarded to emi officer

Sensitive Data

Home

Big Data

Bank Officers Authentication Page

Authenticator Name

clerk

Password

\*\*\*\*\*

Submit Query

Sensitive Data

Home

View Status of Bank Employee

Back

Big Data User Authentication Page

Record Details

Candidate Records


Select

File Details




Nationality	Indian
Reference No	7709
FirstName	amarash
LastName	devaraj
Par_No	4567890987
Mobile	9087890987
Dob	2.3.1990
Gender	male
curr_residential_address	westmardalam
curr_residential_phone	04142-298678
permanent_address	westmardalam
permanent_phone	04142-255768
gross_income	7088e71e9ab6e0ab4252760579ade0f1






Gender	male
curr_residential_address	westmambalam
curr_residential_phone	04142-299878
permanent_address	westmambalam
permanent_phone	04142-255768
gross_income	708be71b9ab6e0a84252760579ade9f1
existing_loan_amount	03e6c61603f6c550ab49ab6a2d83f793
existing_curent_outstanding	1bd69c7df3112fb9a584fbd9edfc6c90
existing_balance_tonor	e93028bdc1aacdfb3687181f2031765d
loan_amount	2a3a2d28294f5c0cf89b066a8d0f9e17
emi	ce774d9cab3ae0bdf522cd0839bed364
declation_name	amaresh



[Verify](#)

   http://localhost:8084/sensitive/clerk\_verify.jsp?loan\_no=7709

 Insert title here  

\*\*\*\*\* Application will be verified by clerk \*\*\*\*\* [Back](#)


Now the request that is forwarded by the clerk will be in the bending list of the emi officer and the values that are encrypted for the clerk will be visible to emi officer

Sensitive Data

Home

Big Data

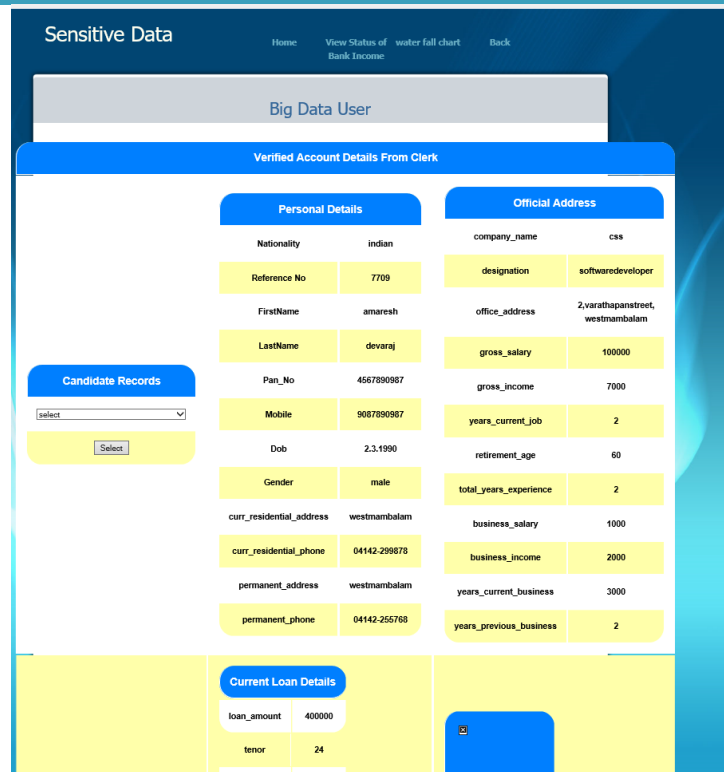
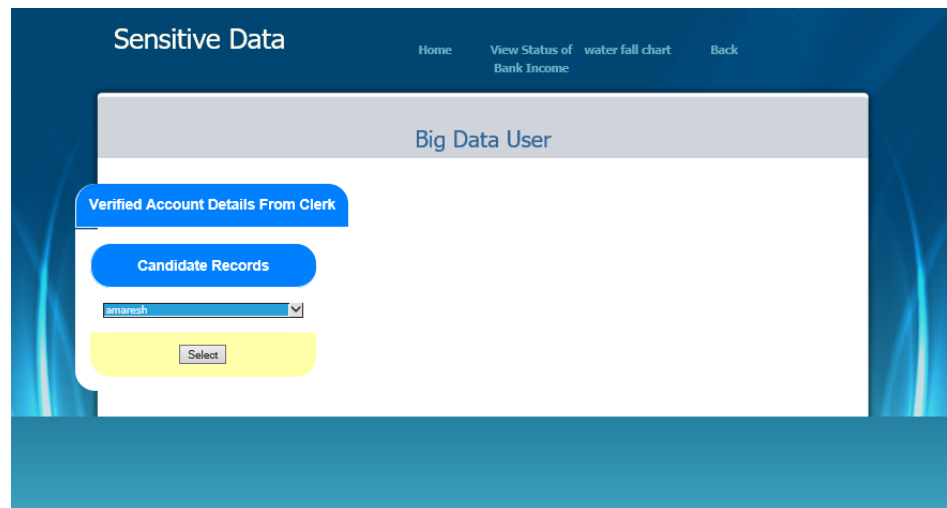
Bank Officers Authentication Page



Authenticator Name

Password

[Submit Query](#)



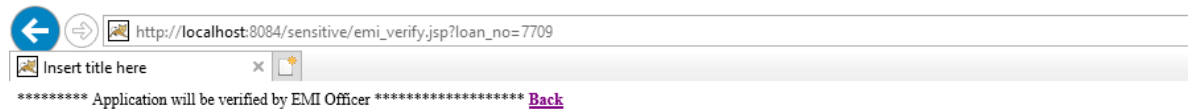
Select		Dob	2.3.1990	retirement_age	60
Gender	male			total_years_experience	2
curr_residential_address	westmambalam			business_salary	1000
curr_residential_phone	04142-299878			business_income	2000
permanent_address	westmambalam			years_current_business	3000
permanent_phone	04142-255768			years_previous_business	2

Current Loan Details	
loan_amount	400000
tenor	24
enduse	UHIM
signature	amaresh
emi	SI

Verify

Now after verification it is forwarded to the loan approval officer snapshots are given below



Sensitive Data

Home

Big Data

Bank Officers Authentication Page

Authenticator Name

loan\_approval\_officer

Password

\*\*\*\*\*

Submit Query

Sensitive Data

[Home](#)
[Bank Income](#)
[Bank Year calculation](#)
[Back](#)

Big Data User Authentication Page

Record Details

Candidate Records

Verified Account Details From Clerk

Salary Details

gross_salary	100000
gross_income	7000
years_current_job	2
retirement_age	60
total_years_experience	2
business_salary	1000
business_income	2000
years_current_business	3000
years_previous_business	2

Previous Loan Details

existing_personal_loan	yes
existing_loan_no	24534
existing_institution_name	csa
existing_type_loan	personal
existing_loan_amount	200000
existing_curent_outstanding	4000
existing_balance_tonor	3000

Current Loan Details

loan_amount	400000
tenor	24
enduse	UHM
signature	amareesh
emi	SI

Verify

[←](#)
[→](#)
[🖼️](#)
[http://localhost:8084/sensitive/loan\\_approval\\_verify.jsp?loan\\_no=7709](http://localhost:8084/sensitive/loan_approval_verify.jsp?loan_no=7709)

[🖼️](#) Insert title here

\*\*\*\*\* Application will be verified by Loan approval officer \*\*\*\*\* [Back](#)

Sensitive Data

Home

Big Data

Bank Officers Authentication Page



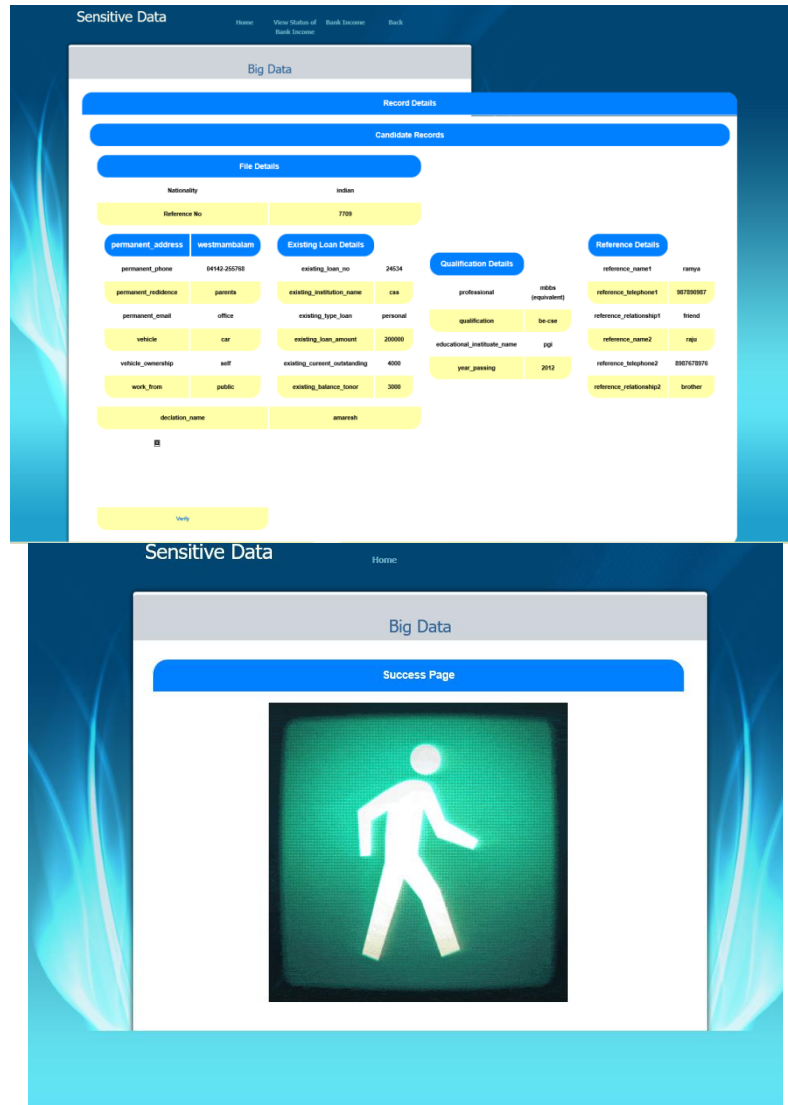
Authenticator Name

bank\_manager

Password

\*\*\*\*\*

Submit Query



- At last the main values that are needed for the loan approval are forwarded to the manager and after final checking the loan amount will be approved

## 7. Conclusion

we proposed a methodical construction of secure sharing of fragile data on huge data stage, which ensures secure convenience and limit of delicate data reliant upon the heterogeneous middle person re-encryption computation, and guarantees secure usage of clear substance in the cloud stage by the private space of customer measure subject to the VMM. The proposed structure well guarantees the security of customers' tricky data. At the same time the data owners have the limitless oversight of their own data, which is a potential response for balance the upsides of included social events under the semi-trusted in conditions. Later on, we will redesign the heterogeneous go-between re-encryption computation, and further improve the capability of encryption. Furthermore, diminishing the overhead of the relationship among included social affairs is in like manner a huge future work

## 10. Future Work

The undertaking has covered practically every one of the necessities. Further prerequisites and enhancements should handily be possible since the coding is principally organized or particular in nature. Enhancements can be affixed by changing the current modules or adding new modules. One significant advancement that can be added to the venture in future is secure record in partitioning hub, which is by and by accomplished for duplicated documents.

## **11. References**

- [1] J. D. Preece and J. M. Easton , Towards Encrypting Industrial Data on Public Distributed Networks Date Added to IEEE Xplore: 24 January2019
- [2] Thanh Dat Dang, Doan Hoang, and Diep N. Nguyen , Trust-based Scheduling Framework for Big Data Processing with MapReduce , Added to IEEE Xplore:September
- [3] Mansukhdeep Kaur, Mohnsin Murtaza, Mostafa Habbal, Post study of Blockchain in smart health environment Networks Date Added to IEEE Xplore: March 2021
- [4] Yu Jin, Chuan Tian, Heng He1, Fan Wang, A Secure and Lightweight Data Access Control Scheme for Mobile Cloud Computing , Date Added to IEEE Xplore: October2015.
- [5] Xinhua Dong, Ruixuan Li, ~~Heng He, Wanwan Zhou,~~ Zhengyuan Xue, and Hao Wu , Secure Sensitive Data Sharing on a Big Data Platform, : March 2018
- [6] Lloyd Greenwald , Kurt Rohloff and David Stott, Secure Proxy-Reencryption-based Inter-network Key Exchange, Date Added to IEEE Xplore: September2018
- [7] Rizky Putri Meiliasari, Amril Syalim, and Setiadi Yazid , Performance Analysis of the Symmetric Proxy Re-encryption Scheme Date Added to IEEE Xplore: Date of Conference: October2019
- [8] Zhanwen Chen, Jiageng Chen, Weizhi Meng, A New Dynamic Conditional Proxy Broadcast Re-Encryption Scheme for Cloud Storage and Sharing, Date Added to IEEE Xplore: Date of Conference: November2020.
- [9] Bharati Mishra, Debsish Jena , CCA Secure Proxy Re-Encryption Scheme for Secure Sharing of Files through Cloud Storage, Date of Conference: January2018.
- [10] Yu Zhan , Baocang Wang , Zheng Wang, Tao Pei, Yuan Chen, Quanbo Qu, and Zhili Zhang, Improved Proxy Re-Encryption With Delegatable Verifiability , Date of Conference: May201

