Enabling Identity-Based Integrity Auditing and Data Sharing with Sensitive Information Hiding for Secure Cloud Stoage

Tanmay Joshi[1†], Asha S[2††]

School of Computer Science and Engineering & Centre for Cyber Physical Systems
Vellore Institute of Technology, Chennai, India

Abstract

With the increase in the data growth, where data storage becomes difficult if the user wants to store it on a local drive, which is why many organizations and people prefer storing their data on a cloud storage. With accessibility of cloud storage, people can remotely use cloud storage and avail data storage. To guarantee the integrity of data stored in clouds, remote data integrity has been proposed. One example of cloud storage is health care system, where the cloud file might have sensitive information. This sensitive information should not be shared with others. One solution would be to encrypt the whole file so avoid sensitive data sharing, but then this way the file would be unusable to others. The method of realizing data sharing with sensitive information hiding in remote data integrity auditing is one sector that has not been explored yet. To do so, we are going to develop a sanitizer which will sanitize blocks of data corresponding to sensitive information of the file, and transform these data blocks signatures into valid ones for the sanitized file. These signatures are used to validate the sanitized file in the phase of integrity auditing. As a result, this scheme allows files to be shared with others, while also maintaining data security by sanitizing blocks of sensitive data, with the data integrity auditing still able to be executed efficiently without any problems. The proposed system is based on identity-based cryptography, which simplifies complicated certificate management. The security analysis and the performance evaluation show that the proposed scheme is secure and efficient.

Keyword:
Healthcare, data, storage, security, integrity, cloud, information

1. INTRODUCTION

An important sector of online healthcare system is cloud computation. Tawalbeh proposed a system for mobile application which automatically analyses the patient records and can extract auto-recommendations. The healthcare system requires more increasingly resources for communicating and computing, which requires data access in and out of the organization itself. The higher version of healthcare applications are bound to be able to communicate with each other outside of their organization's boundaries. We briefly discuss the power of cloud computation in the healthcare industry that shows how reliant is the healthcare system on technology based on cloud computation. The rapid arrival and emergence of cloud computation, IoT, and massive data technology are transforming health and all Industry into health applications. The Health Industry allows for increased flexibility in a variety of aspects including production, accelerated both production and processing market, betterment of quality of product and production, and transform business models that transform communication and price connections, competitors and customers. Hospitals and doctors choose certain strategies to increase business flexibility, while deducting the cost of large amounts of health care. Therefore, cloud-based computing is rising in health care as doctors, hospital admins and clients seek cost-effectiveness, and hands on availability to information.

The current objective of healthcare industry is on cloud computation, reasoning being it helps to achieve various goals such as access to infrastructure. Cloud computation can help in reducing production price as it removes the need to duplicate hardware locations at each hotspot. It helps in transforming healthcare system. It also helps in the delivery of collaborative and group healthcare and the ability to use applications constructed on the needs of the business model and some medical data. All this can be executed on a platform where the industry can deliver and implement, and finalize new features depending on a holistic and intellectual perspective of clients regardless of whosoever the care was provided.

"This will require maintaining a level of security and privacy equal to or greater than that provided by traditional IT. In distributed mobile cloud computing (MCC), mobile users receive cloud server data from various servers using a mobile App or web browser. The MCC environment is made up of a variety of mobile users and multiple cloud-based servers. These cloud servers can contain a wide variety of data signals, which can be accessed by a wide range of mobile users. Interestingly, these cloud data attributes have a very different nature. There may be some server data restrictions restricted to only authorized users. Therefore, it requires the control of good access to data signals for multiple servers. Integrated access control gives access to a specific user with a certain right. Over the past few years, researchers have made a unique contribution to

Manuscript received December 5, 2024
Manuscript revised December 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.12.18

building user authentication for multiple servers and managing explicit access to data stored on cloud servers. In light of the previous work of Key-Policy Attribute-based Encryption (KP-ABE), good access control schemes have been proposed in recent years, designed for a variety of programs: wireless sensor network (WSN) security cloud security and e-health care system."

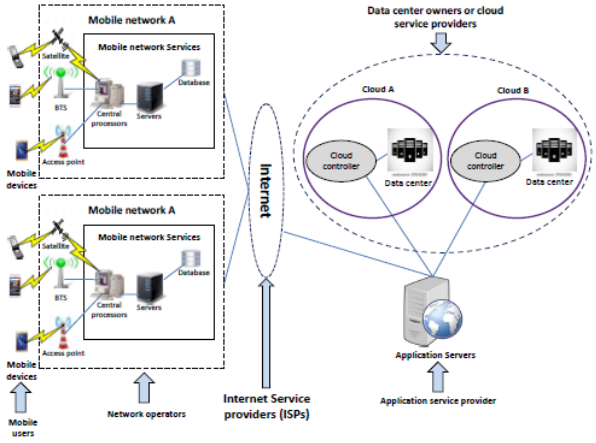

Fig. 1. An architecture for distributed mobile cloud computing

It is important to consider user authentication methods for for mobile cloud computing, which is elaborated in this report. So, mobile users keep getting could server data over a not so secured open channel, a secure verification of interaction is needed where cloud servers can be bridged with mobile users. Watching the state of the user's device resources, the configuration of this verification process should be simple enough. A small literature study of authenticity of mobile cloud computation shows that there is lack of significant work which hasn't been done on building a strong data access control for multi-cloud data. All available finefinched-related access control schemes are designed for one location only. Prior to granting access to its data signals, the entire CSj cloud server needs to confirm the legitimacy of mobile user. A true MUi user can get hands on the CSj server data details, if they have the appropriate access right or access permission as set by the appropriate server.

2. Existing System

In our current system use secure encryption for cloud data. Specifically, it aims to achieve two goals that are, integrity of data and removal of duplicates in the cloud, using programs which are SecCloud and SecCloud +. SecCloud introduces an auditing entity with MapReduce cloud storage business, which helps clients generate data tags before uploading and check the integrity of data stored in the cloud. SecCloud + is designed to promote that the clients can encrypt their data before deciding to transfer their data to cloud, and allows to audit integrity of data along with removal of duplicate encrypted data.

3. Drawback

• "Remote data integrity schemes cannot support data sharing by encrypting sensitive information.
• Cannot reduce computation overhead

4. Proposed plan

In our proposed program a data integrity research scheme is proposed that recognizes data distribution by encrypting sensitive information. cloud, user, sanitizer, Private Key Generator (PKG) and Third Party Auditor (TPA).

(1) Cloud: Cloud provides huge storage space for the user. With the cloud storage service, users can upload their data to the cloud and share their information with others.
(2) User: User is a member of an organization, with a large number of files to be stored in the cloud."[2]
(3) Sanitizer: The sanitizer is responsible for the sanitization of the data associated with sensitive information (personal and organizational sensitive data) in the database, converting these data signatures into valid file signatures, and and uploading the final sanitized file with the generated digital signatures to the cloud.
(4) PKG: Packet key generator is trusted by other organizations. It is packet key generator's work to create the file's public parameters and the client's private key based on his identification.
(5) TPA: Third party auditor is responsible for open verification. Third party auditor is responsible for maintaining data integrity while uploading the corresponding file to the cloud for the clients.

Benefits:

• Reduce computation power
• Reduce transfer costs between public cloud and data users

5. Module Description

Registration Center:
"Prior to deploying CSj cloud servers, stores required information such as server id, master key, cyclic group and generators on the corresponding servers."

File Upload:
After registering RC can upload a file with access policy. If any attribute of the cloud server is satisfied with the access policy they can access the file using the crypto key.

Mobile User Registration:
"MUi signs-in to RC through a secure channel by selecting their qualifications. RC selects user server interaction parameters and data loads required in the user's smart id."

Sign-in Authentication:
MUi transports its data and uses the limits stored on the smartcard to log in to the cloud server CSj you want. MUi does not use different data to sign in to different cloud servers.

User authentication and authorization phase:
"At this stage, CSj verifies the authenticity of the intended MUi user, and sends its own set of data responsibilities and encrypted keys. MUi is able to encrypt this key, therefore, it can only establish a share session key if it has the appropriate access permission."

System Architecture Diagram:

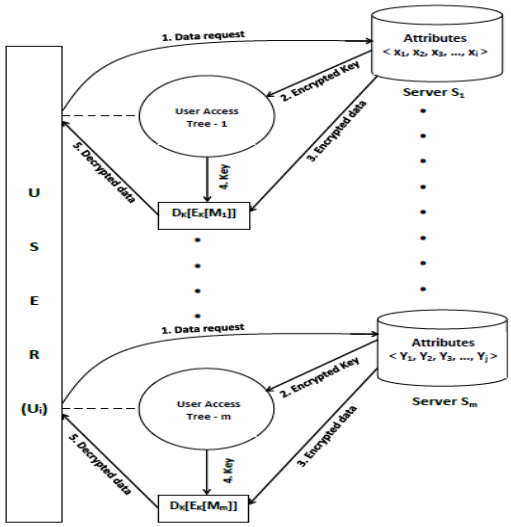

Fig 2. System Architecture Diagram

6. FEASIBILITY STUDY

"Project feasibility is analyzed at this stage and the business proposal is based on the most common project plan and other cost estimates. During the analysis of the plan a study will be conducted on the feasibility of the proposed system. This is to ensure that the proposed system is not a burden to the Network user. Accurately identified credit card fraud in store stores. The analysis of the feasibility, a certain understanding of the major needs of the system is essential.
The three basic considerations involved in the analysis of probability are these"

- ECONOMICAL FEASIBILITY
- TECHNICAL FEASIBILITY
- SOCIAL FEASIBILITY

Flow Diagram:

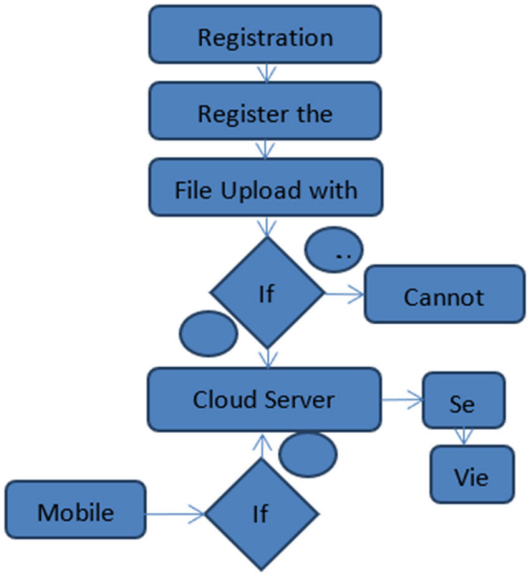

Fig 3. Flow Diagram

Economical Feasibility
"This study was done to look at the economic impact it would have on the organization. The amount of money a student can contribute to research and program development is limited. Expenses must be allowed. The improved system is therefore in the middle of the budget and this has been achieved because most of the technology used is freely available."

Technical Feasibility
"This study was conducted to look at the feasibility of technology, that is, the technical needs of the system. Any plan made should not have a high demand for available resources. This will lead to higher demand for available technical resources. This will result in higher demands being placed on the client. The improved system should have a modest need, as few or no changes are required in implementing the system."

Social Feasibility

"The study feature is to assess the level of acceptance of the system by the user. This includes the process of training the user to use the system properly. The user does not feel threatened by the system, instead should accept it as a necessity. The level of user acceptance depends only on the methods used to educate the user about the program and get him or her acquainted with it. His level of self-confidence should be enhanced so that he can make constructive, well-received criticism, as he is the last user of the program."

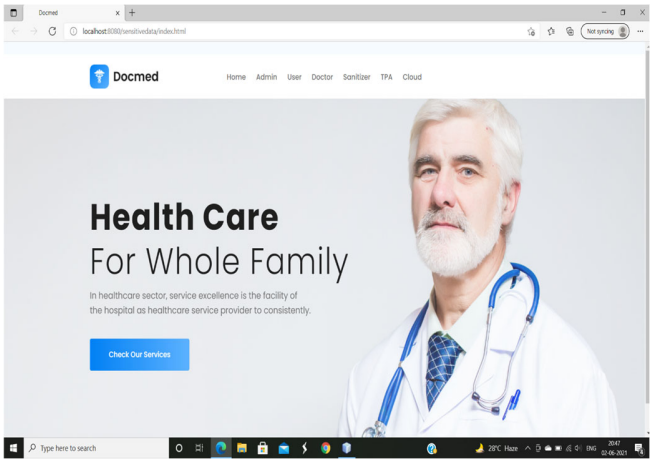

Fig 4 Home Screen

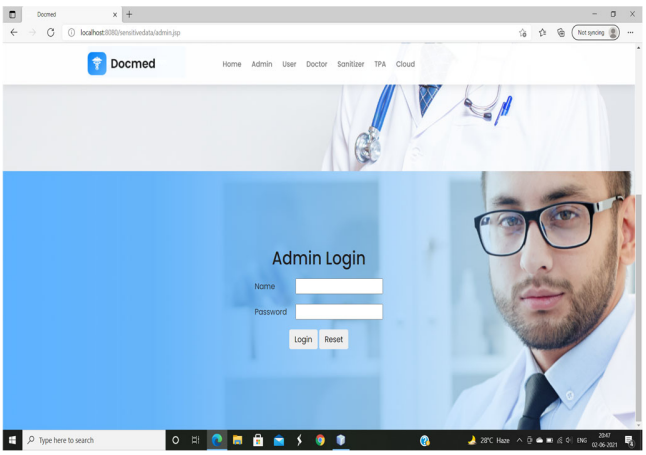

Fig 5 Admin Login Screen

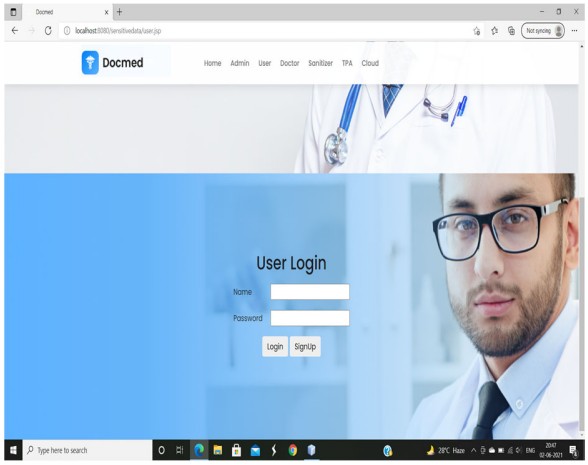

Fig 6 User Login Screen

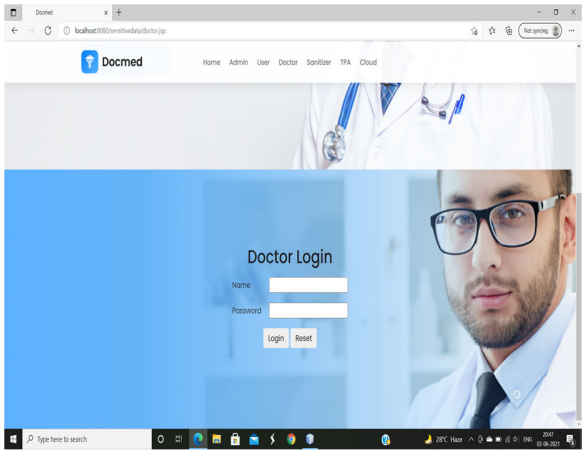

Fig 7 Doctor Login Screen

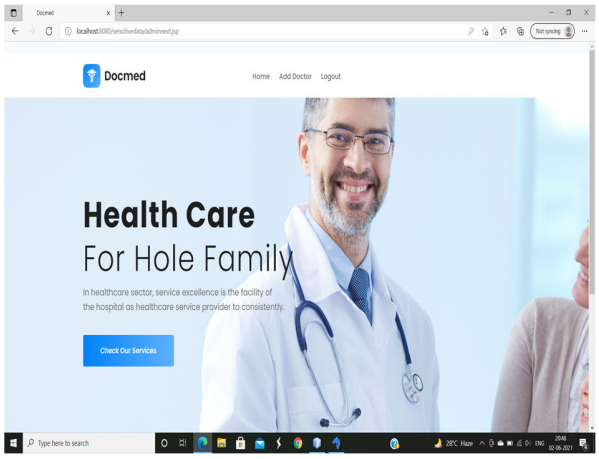

Fig 8 Admin Screen

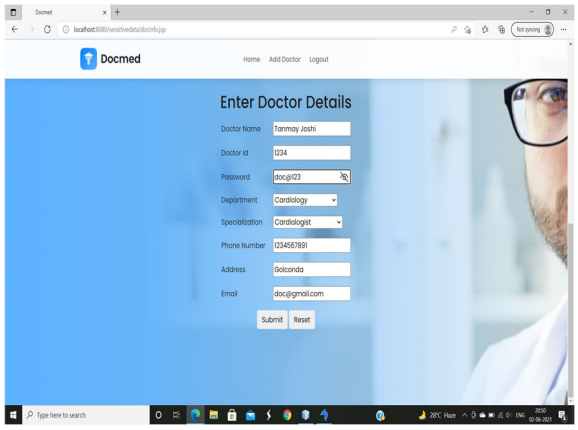

Fig 9. Add Doctor Screen

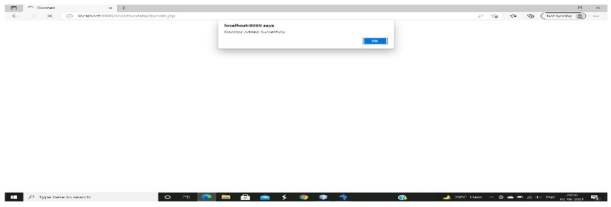

Fig 10 Doctor Added confirmation box

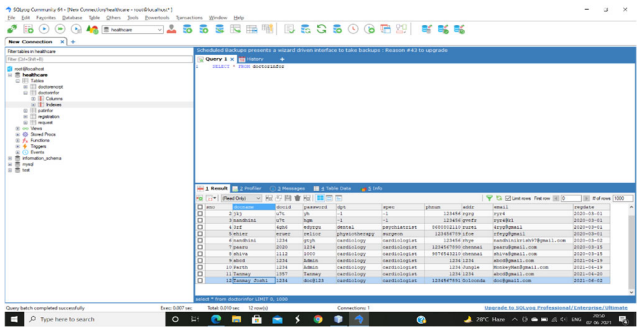

Fig 11 Healthcare System Database

7. CONCLUSION

Mobile cloud computing is in desperate need of a fine-grained, multi-server access-level of control over the cloud. From the fine-grained ability to manage a huge cloud server is a problem to the environment on which more research can be done. In this article, we are presenting a new development framework that provides a combined fine-grained approach to the cloud for the control of multi-server data, in conjunction to a probably safe user authentication. Another field of research could be on the authentication process to reduce computation overhead of cryptography for systems that have limited battery life such as mobiles or laptops. Since the proposed scheme isn't having the RC in the identification procedure, it also has a lower communication cost compared with the existing systems.

8. FUTURE WORK

In our future work focus to improve the authentication technique in login process by using the negative password model. In order to avoid the replay and rainbow attack. In our future work, we can add a search query for advanced data retrieval queries. In this way we use the lazy and merged approach to analysis and obtain a question record-based answer on the cloud data.

REFERENCES

1. artemis.library.tuc.gr [1]
2. artemis.library.tuc.gr [2]
3. docplayer.net [3]
4. Sandip Roy, Ashok Kumar Das, Santanu Chatterjee, Neeraj Kumar, Samiran Chattopadhyay, Joel Jose Rodrigues. "Provably Secure Fine-Grained Data Access Control over Multiple Cloud Servers in Mobile Cloud Computing Based Healthcare Applications" , IEEE Transactions on Industrial Informatics, 2018 [4]
5. www.componentsource.com [5]
6. www.rankly.com [6]

Tanmay Joshi
Tanmay is Under Graduate Engineering Student of Vellore Institute of Technology. His areas of interest include networks security and programming.

Asha S
Asha is Associate Professor at Vellore Institute of Technology, Chennai. She is the member of the Centre for Cyber Physical Systems. She received her doctorate from Anna University and Master's degree from SRM University. She had published more than 30 research papers to her credits. Her area of interest includes biometrics, network security, IoT, blockchain and Cyber Physical Systems.