Authentication of Medical Documentation with Privacy Protection and Sharing in Cloud

Sneha Y S[1], Shivamurthy R C[2]

[1]M.Tech. Student, CSE, Maharaja Institute of Technology, Mysore
[2]Professor & HOD, CSE, Maharaja Institute of Technology, Mysore

ABSTRACT

There is a growing need for better medical care as a result of the adoption of clever electronic gadgets and the development of cloud and cloudlet technologies. Data collection, storage, and dissemination are the three main steps in the medical data processing chain. The traditional healthcare system frequently requires the transfer of medical data to the cloud, resulting in the use of sensitive user data and communication energy. The exchange of medical information is a crucial and difficult problem. In this study, we suggest a brand-new human services framework that makes use of cloud let's flexibility. Security assurance, information sharing, and intrusion detection are among the components of cloudlets. We apply the Number Theory Research Unit (NTRU) technique to encrypt the user's bodily data gathered by wearable devices during the data gathering phase. This information is then efficiently transferred to nearby cloudlets.

We also present a trust model to help users choose reliable partners that want to share cloudlet-stored data.

INTRODUCTION

Overview

In the world of cloud computing, the authority is in charge of accepting user enrollment and setting up certain guidelines. The cloud service provider (CSP) looks after the cloud servers and provides customers with a range of services.

The data owner encrypts the ciphertext produced and then uploads it to the CSP. The user then downloads the required ciphertext from the CSP and decrypt it.

The standard set up of shared files is characterized by a hierarchical structure, where a department's collection of files is separated into a number of sub-departments that are organized in a hierarchical fashion and have varied levels of access.

It would be more cost-effective for both parties if the files in the same hierarchical structure were encrypted using an integrated access structure.

Through the use of cloud computing, clients with limited computational resources can transfer their heavy computation workloads to the cloud, where they can take advantage of the significant computational power, bandwidth, storage, and even suitable software that can be shared on a pay-per-use basis. A cutting-edge paradigm for computing, cloud computing enables flexible, on-demand, and cost-effective use of computing resources.Due to the fact that the information belonging to different customers is stored on cloud servers rather than being in their direct control, the points of interest in issue unanticipated give rise to security and protection concerns.

Unresolved are the security issues surrounding cloud computing. Several Attribute-Based Encryption-based techniques have been used to overcome these issues.Particularly speaking, workloads for outsourced computing frequently contain sensitive data, such, but not limited to, commercial financial records, confidential research data, or personally identifiable health information. Sensitive data must be encrypted before outsourcing in order to guarantee end-to-end data protection in the cloud and beyond and stop unauthorized information leaking. Computation over encrypted data is a difficult problem since traditional data encryption techniques often restrict the cloud from carrying out any important operation of the principal computation content arrangement.

Due to its dynamic structure, the suggested plot provides a great level of adaptability. In the area of public social distributed computing, we offer secure protection. With three hierarchical levels—Cloud Specialist, Domain Expert, and Users—our concept integrates a ground-breaking property-based security framework. The private cloud expert domain can be added or removed by the cloud specialist, who is also in charge of maintaining all the information in the overall cloud. On the other hand, the Domain Expert has the authority to add or remove private users from the domain.

Motivation

A sizable amount of information is released or shared daily in the context of information societies. The potential for the publication of medical records to improve the calibre and efficacy of healthcare services has made this case of information release stand out among others. However, in later applications, it is crucial to guarantee the authenticity and integrity of released medical documents. Furthermore, when medical records are made accessible to unreliable parties without sufficient management, the sensitive nature of most of this information poses a major threat to privacy.

With redactable signatures, any party has the option to remove specific sections of an authenticated document while still maintaining the subdocument's integrity and provenance. The majority of currently used redactable signature systems (RSSs) are, however, vulnerable to dishonest redactions or unlawful redaction detection. We suggest two different RSSs with flexible release control (RSSs-FRC) to solve these problems. We also evaluate how well our buildings operate in terms of security, effectiveness, and functionality. Our investigation' findings show that, in terms of efficiency and security, our constructions provide a significant advantage over those of competitors.

Problem Statement

Fuzzy Identity-Based Encryption (IBE), which served as the forerunner to Attribute-Based Encryption (ABE), was a concept developed by Sahai and Waters in 2005. A BE version called as CP-ABE was subsequently suggested. Numerous hierarchical CP-ABE methods have been proposed since Gentry and Silver berg first suggested hierarchical encryption schemes. For instance, Wan et al. provided a hierarchical ABE scheme, while Wang et al. developed a hierarchical ABE system that incorporated hierarchical IBE and CP-ABE. Later, Zou presented a hierarchical ABE method with a linearly correlated secret key length to the attribute set order. Further research has been done on a hierarchical ABE system with brief ciphertext. In these schemes, a top-level authorization domain generates the secret key of the next-level domain, and the parent authorization domain controls its child authorization domains. Multiple authorization domains share the burden of key creation, which lessens the workload placed on the key authority centre.

Objectives

The challenging problem of safe data sharing in cloud computing has given rise to the popular encryption approach known as cypher text-policy attribute-based encryption (CP-ABE). In industries like healthcare and the military, shared data files frequently show a multilayer hierarchy. However, in the context of CP-ABE, the hierarchical structure of shared files has not been fully investigated. An effective file hierarchy attribute-based encryption technique for cloud computing is suggested in this paper.

To encrypt hierarchical files, the technique combines multilayer access structures into a single access structure. The files can share the ciphertext components relevant to the characteristics, which saves on both ciphertext storage and encryption time. The suggested approach has also been shown to be secure under common assumptions. Experimental simulations show how effective the suggested approach is at both encrypting and decrypting data. The benefits of our plan become more and more clear as the quantity of files rises.

PROPOSED SYSTEM

Online data sharing has become increasingly common due to the spread of network technology and mobile devices, as seen by websites like Facebook, MySpace, and Badoo. In this situation, cloud computing has shown promise as a platform for application development to deal with the exponential expansion of data sharing.

Users must encrypt their data before sharing it with others in order to guarantee data security in cloud computing. Access control is crucial because it protects shared data from unauthorized access by acting as the first line of defence.

Because it allows for precise, one-to-many, non-interactive access control while preserving data privacy, attribute-based encryption (ABE) has recently attracted a lot of attention.

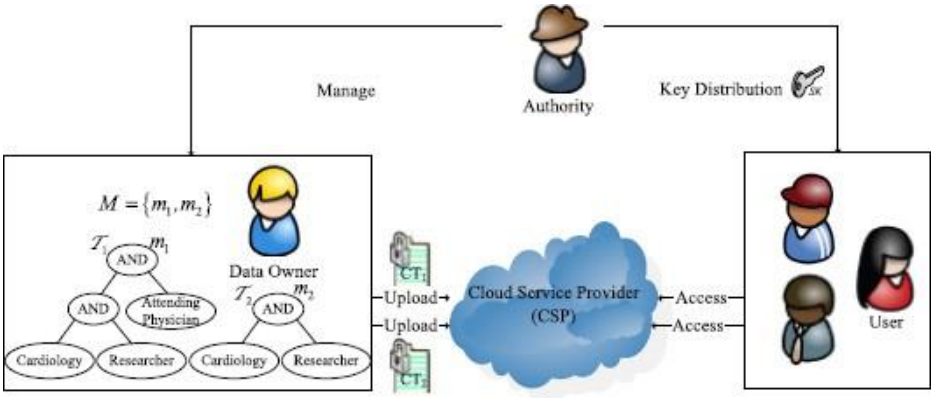


Figure: **Attribute Based Encryption**

A workable encryption method that provides more flexibility and is better suited for all cloud computing applications is cypher text-policy attribute based encryption (CP-ABE). The authority is in charge of accepting user membership and establishing numerous settings, as shown in Figure 1. The cloud service provider (CSP) oversees the cloud servers and offers clients a variety of services. The user downloads and decrypts the desired ciphertext from the CSP once the data owner encrypts and uploads the created ciphertext to the CSP. Shared files typically have a hierarchical structure, where a set of files is broken up into multiple subgroups with varying levels of access. The cost of ciphertext storage and processing time can be reduced if the files contained in the same hierarchical structure can be encrypted using an integrated access structure.

In order to safely share PHR data in the cloud, a patient may separate their PHR data M into two parts: personal data m1, which might comprise the patient's name, social security number, contact information, home address, etc.Sensitive personal data, such as test results, treatment plans, and operation notes, are absent from the medical record designated as m2. The patient then uses the CP-ABE technique to encrypt the data in m1 and m2 while utilizing different access restrictions that are in line with the real need. For instance, whereas a medical researcher only needs access to certain medical test findings for academic purposes in the relevant field, an attending physician needs access to the patient's name and medical record to help with diagnosis. It is important to remember that a researcher in medicine must also be a doctor, while the opposite is not always true.

METHODOLOGY

SYSTEM ARCHITECTURE:

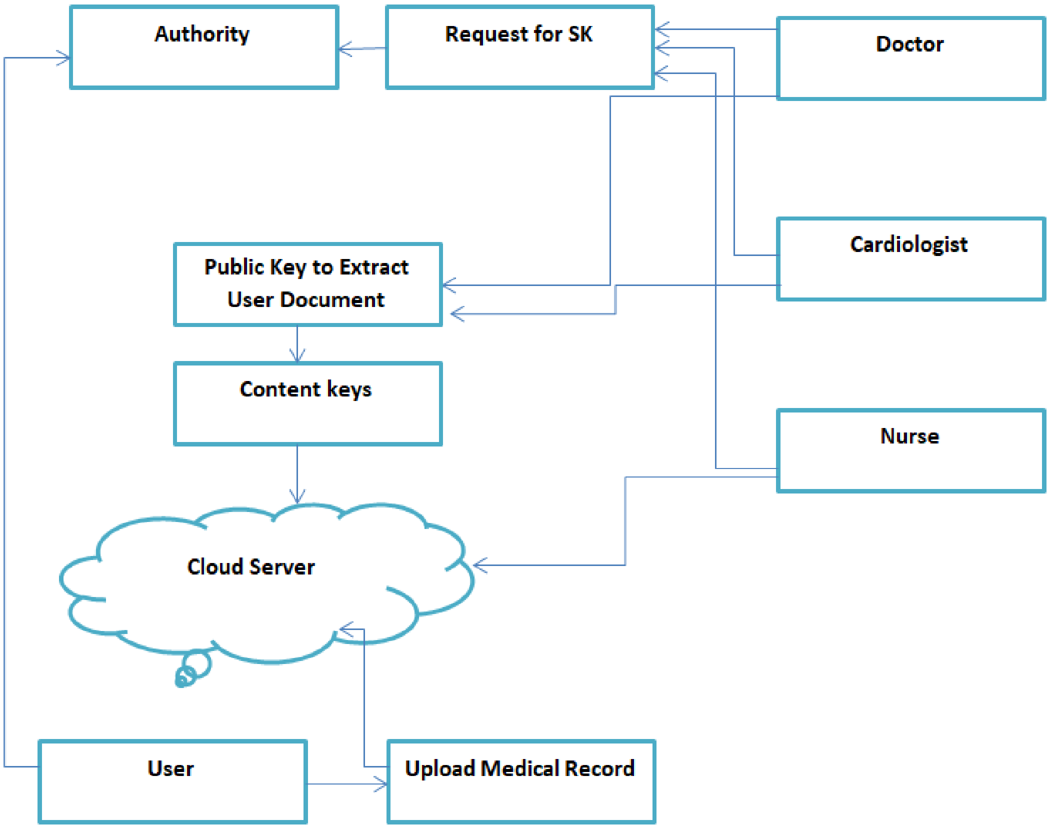


Figure:**System Architecture**

The effective encryption method for cloud computing presented in this work is based on a layered model of the access structure. In order to accomplish straightforward, adaptable, and fine-grained access control, the suggested approach, known as file hierarchy CP-ABE (FH-CP-ABE), expands the standard CP-ABE with a hierarchical structure of access policy. Our plan offers three different benefits.

First, in order to address the issue of sharing numerous hierarchical files, we suggest the layered model of access structure. With a single integrated access structure, the files are encrypted.

The security of the FH-CP-ABE method against specific plaintext assaults (CPA) is secondarily formalised under the Decisional Bilinear Diffie-Hellman (DBDH) supposition.

Thirdly, we carry out a thorough experiment for the FH-CP-ABE scheme and put it into practise. The simulation findings show that the FH-CP-ABE has a low storage cost and low computational complexity for encryption and decryption.

As a result, the FH-CP-ABE technique we've presented is a useful one for cloud computing's file hierarchy attribute-based encryption.

It is crucial to build a safe and reliable system architecture in order to provide medical document authentication while guaranteeing privacy protection and sharing in the cloud. An overview of the major parts and each of their functions is given below:

User Management and Authentication: -

- ❖ Users must safely register and log in to access the system, including patients and healthcare professionals.
- ❖ Multi-factor authentication: A two-factor or multi-factor authentication system must be put into place in order to improve security.
- ❖ User roles and permissions: Based on user responsibilities, several roles and access levels must be defined.

Encryption and Data Privacy: -

Strong encryption techniques, like AES, must be used to encrypt data both in transit and at rest in order to guarantee data privacy.

- ■ **Key management:** Using a secure key management system is advised in order to generate, store, and rotate encryption keys.
- ■ **Data anonymization:** It is advisable to use anonymization techniques while sharing data in order to protect sensitive information while maintaining data utility.
- ■ **Cloud Storage That Is Secure Provider of cloud services:** Selecting a trustworthy and compliant cloud provider is essential. They must offer strong security safeguards and certifications, such as HIPAA for medical data.

Application Programming Interfaces (APIs) must be secured using authentication techniques and access controls if the system makes them available. To guarantee that all security and privacy measures are adequately addressed, it is crucial to include cybersecurity specialists and privacy professionals during the system's design and implementation. The system must also undergo frequent security audits and updates to stay current with the most recent security best practises.

SYSTEM DESIGN AND DEVELOPMENT

Data Flow Design

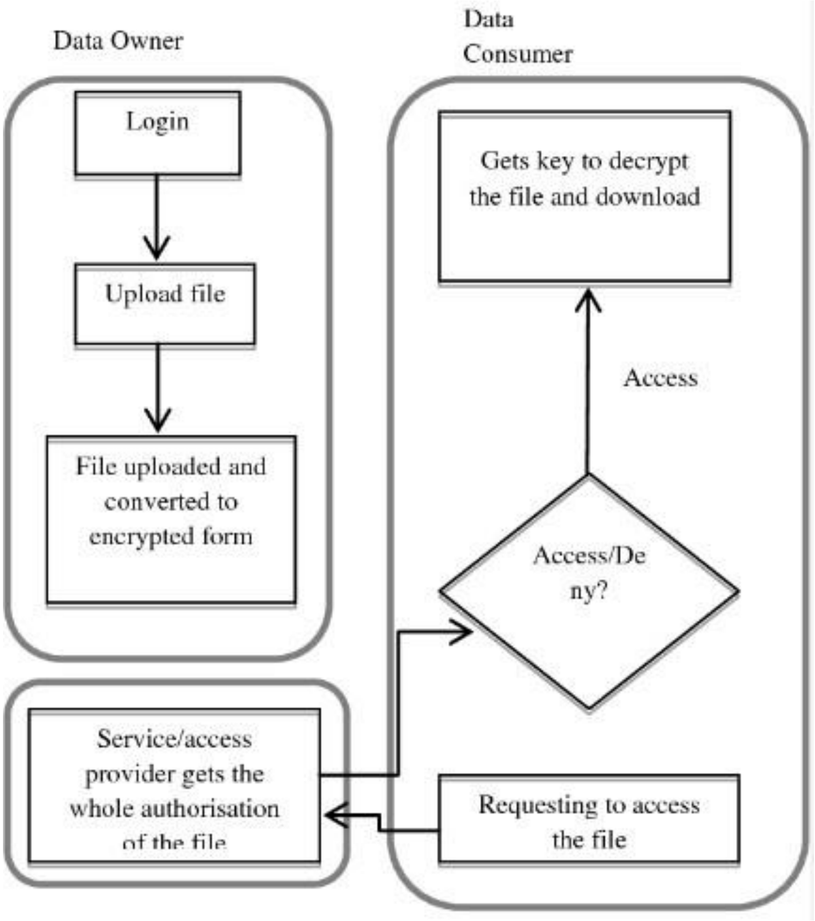

Data Owner
Data Consumer
Login
Upload file
File uploaded and converted to encrypted form
Gets key to decrypt the file and download
Access
Access/Deny?
Service/access provider gets the whole authorisation of the file
Requesting to access the file

Figure: Data Flow

A number of steps and data flow are involved in the authentication of medical documentation with privacy protection and sharing in the cloud to ensure secure access and privacy of sensitive medical information. The process begins with the collection of medical documentation from various sources, such as hospitals, clinics, or individual patients, which is then securely stored in a cloud-based storage system.

Healthcare professionals, patients, and authorized workers who need access to the medical records must first register with the system. They give their credentials, such as their username and password, as well as other authentication elements, like biometric or two-factor authentication, throughout the registration process in order to verify their identity.

Data transit between the user and the cloud server must be encrypted using secure protocols like HTTPS/TLS to prevent eavesdropping and man-in-the-middle attacks. After the user's identification has been confirmed, the system applies access control rules to establish the user's level of access to certain medical records. Users can only access the data that they are permitted to see based on their roles and permissions thanks to access control.

Medical data is extremely sensitive and is governed by stringent privacy laws like HIPAA and GDPR. The system must use a variety of privacy-enhancing methods, such as data anonymization, pseudonymization, or differential privacy strategies, to preserve patient privacy. These techniques assist in lowering the possibility of patient identification while preserving the ability to gain insightful knowledge from the data.

Patients or healthcare professionals occasionally need to exchange medical records with other vetted parties, such insurance companies or experts. The cloud platform enables secure sharing, guaranteeing that only the intended receivers can view the shared information.

The system should generate thorough audit logs that capture all user activity and access attempts in order to preserve accountability and traceability. This data aids in keeping track of and looking into potential security lapses or unauthorized access. To avoid vulnerabilities and safeguard against new attacks, the cloud infrastructure and software need to be updated often with the most recent security patches and standards. The security of the system is continuously monitored to ensure quick identification of and reaction to any suspicious activity.

In conclusion, secure data collection, user registration, authentication, access control, privacy protection, secure sharing, audit trail creation, and ongoing monitoring are all part of the data flow for authenticating medical documentation with privacy protection and sharing in the cloud to ensure the confidentiality and integrity of sensitive medical information.

Encryption flow

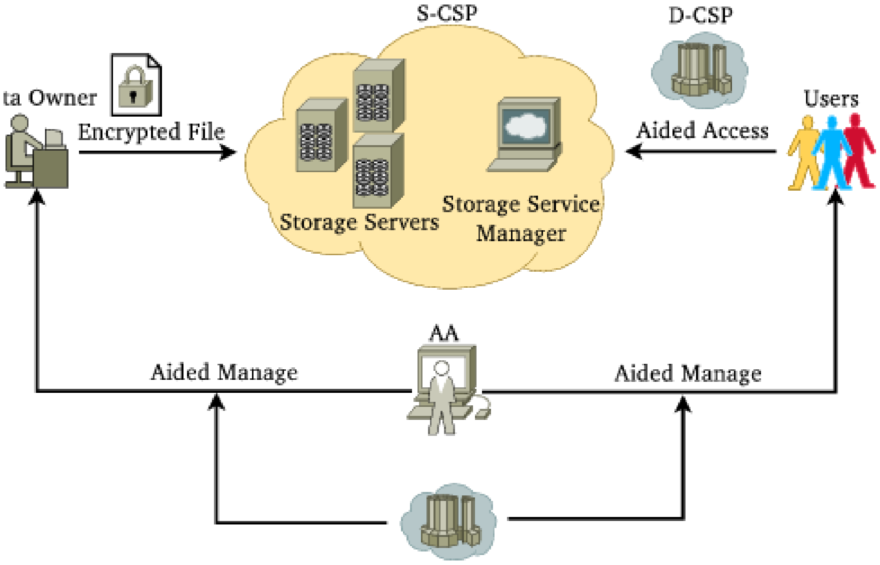


Figure: Encryption Flow

As shown in Figure, we give a suggested structure for cloud storage. The data owner, the cloud server, the data requestor/consumer, and the authority are the four separate parties that make up the framework. The data owner wants to give their information to data requestors controlled by different authorities. Based on the attributes of the consumer or the relevant access policies, each authority generates a secret key for the data requestor within its management domain.

The data owner specifies the desired authorities and the qualities that the data requester should have in the management domains of the relevant authorities before encrypting their file for the data requestors of different organisations, i.e., users governed by separate authorities. The data owner then uploads the encrypted information to the cloud storage server. The cloud server provides the corresponding ciphertext in response to a data requestor's request. If the characteristics labelled with the ciphertext satisfy the access policy connected to the requester's secret key, the requester can decode the data. Otherwise, the requester will be unable to learn anything meaningful about the original data.

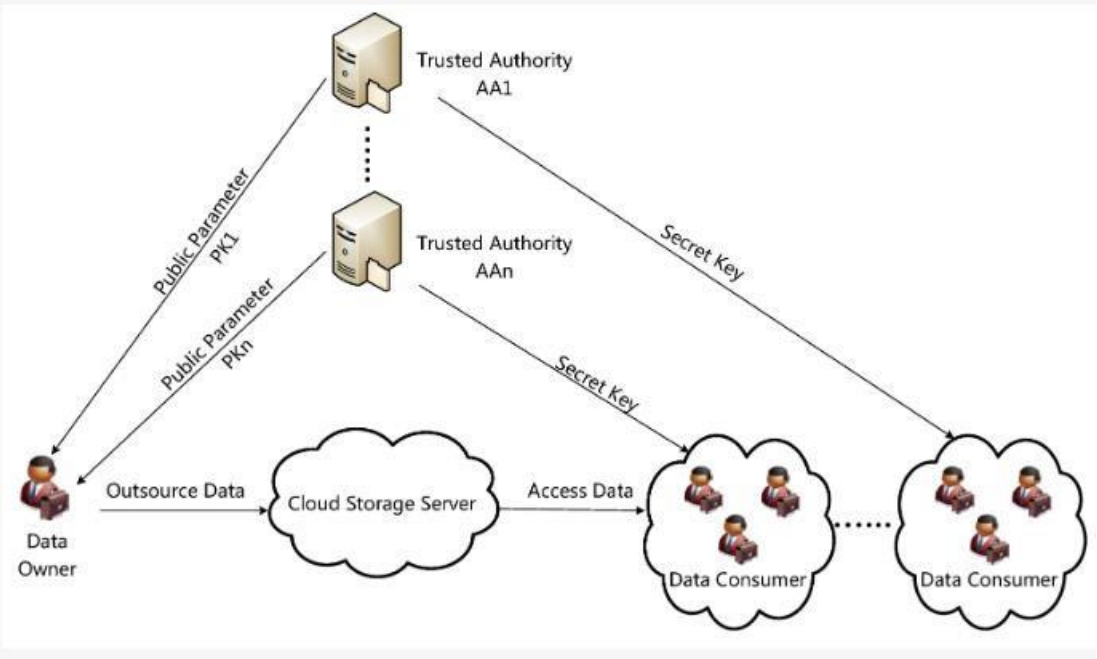


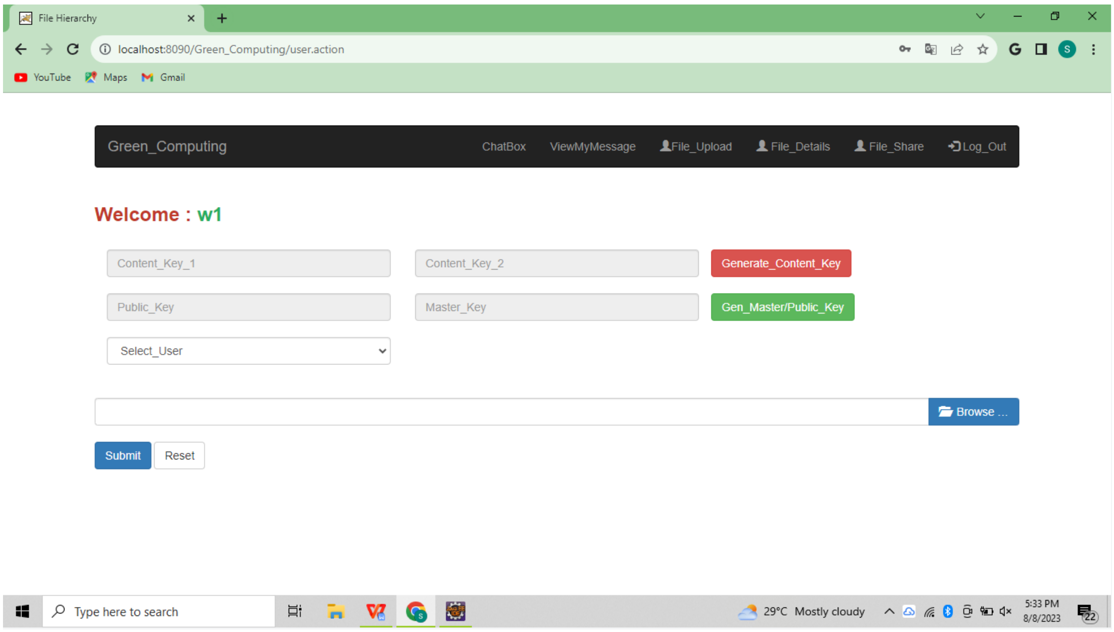
Figure: Batch attribute-based encryption framework

A cryptographic system called batch attribute-based encryption (ABE) enables secure and effective encryption and decryption of data depending on particular attributes related to individuals or the data itself. It offers fine-grained access control, allowing only people with the necessary qualities to have access to encrypted data. By supporting multiple ciphertexts and numerous decryption keys, the Batch ABE framework improves classic ABE schemes and enables more effective operations when dealing with a large number of data items and users.

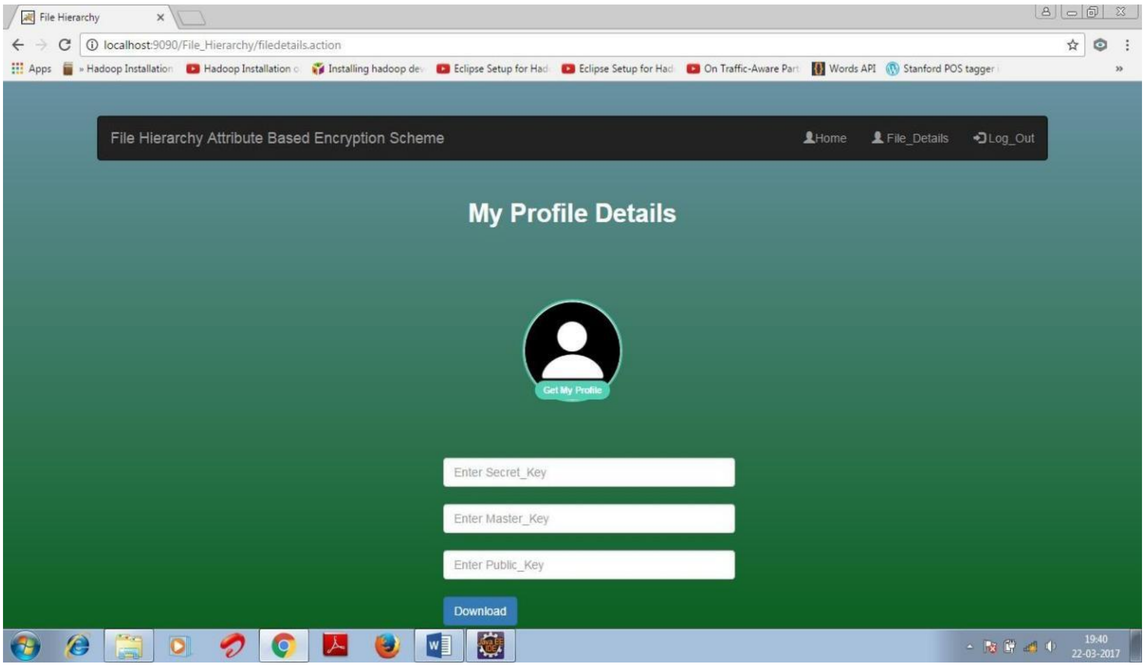
The setup phase, key generation, encryption, decryption, batch operations, and revocation are all components of the Batch Attribute-Based Encryption framework. Public parameters and master keys are generated by a reliable authority during the setup phase. During the key creation step, decryption keys corresponding to authorised users' or entities' attributes are given to them. Data items are encrypted into various ciphertexts during the encryption stage, each of which is connected to a different set of attributes. The data is encrypted in accordance with the access policy or attributes specified by the encryptor. The decryption key matching to the attributes listed in the access policy of the ciphertext must be in the possession of the authorised user in order to perform decryption. The Batch ABE framework's main benefit is its support for batch operations, when several ciphertexts are used.

Various situations where data access needs to be regulated based on user qualities or access regulations, such as secure sharing of sensitive data in a multi-user environment, cloud computing, and secure data outsourcing, find applications for batch attribute-based encryption. It's important to remember that depending on the underlying cryptographic method employed, the precise implementation and mathematical specifics of the Batch ABE framework may change. There may be differences in the security features and efficiency trade-offs offered by various schemes. As with any cryptographic system, the security and effectiveness of the Batch ABE framework in real-world applications depend on rigorous design, analysis, and testing.

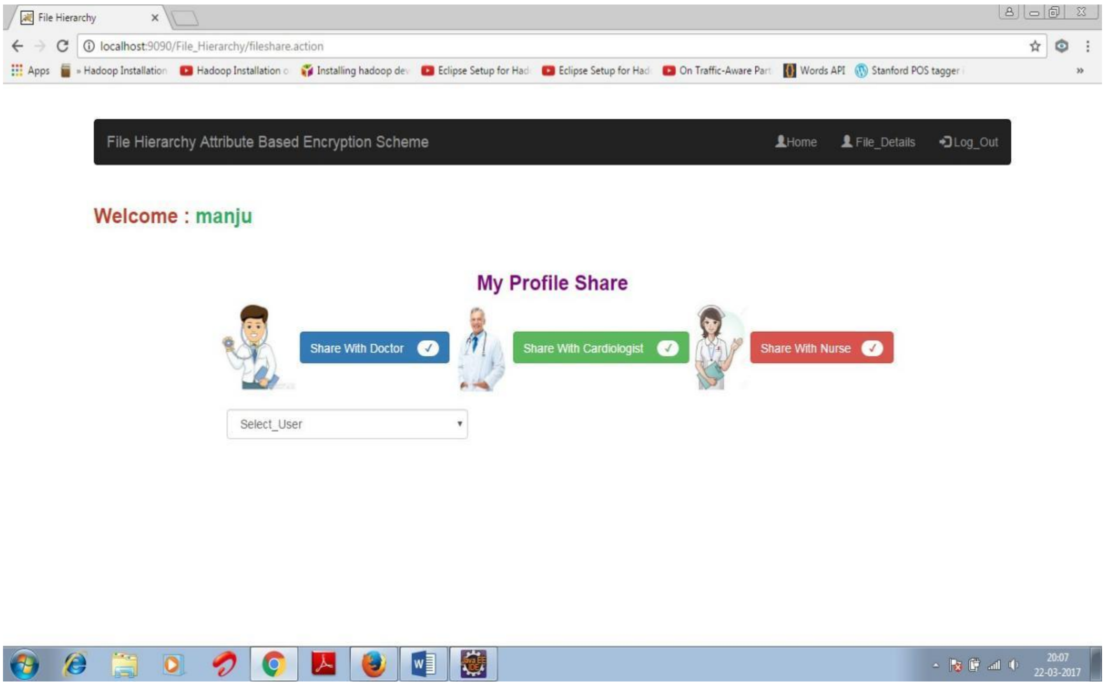
RESULT AND DISCUSSION



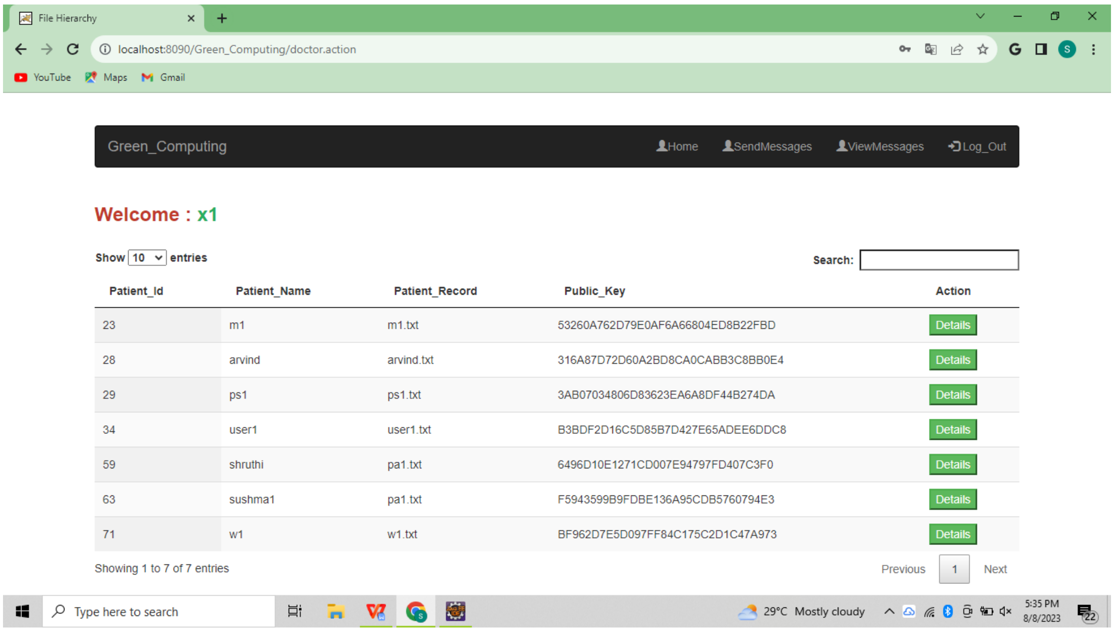
- ✓ In this interface, the user must create a policy and generate content keys in order to upload a file to the target recipient. After that, before the data is uploaded to the cloud server, it must be encrypted using said content keys.



- ✓ The user must enter a secret key, master key, and public key in this window in order to access their data that is kept on the cloud server.



- ✓ This display shows who the data should be shared with, and only people who have been given access are allowed to access the data.



Welcome : x1

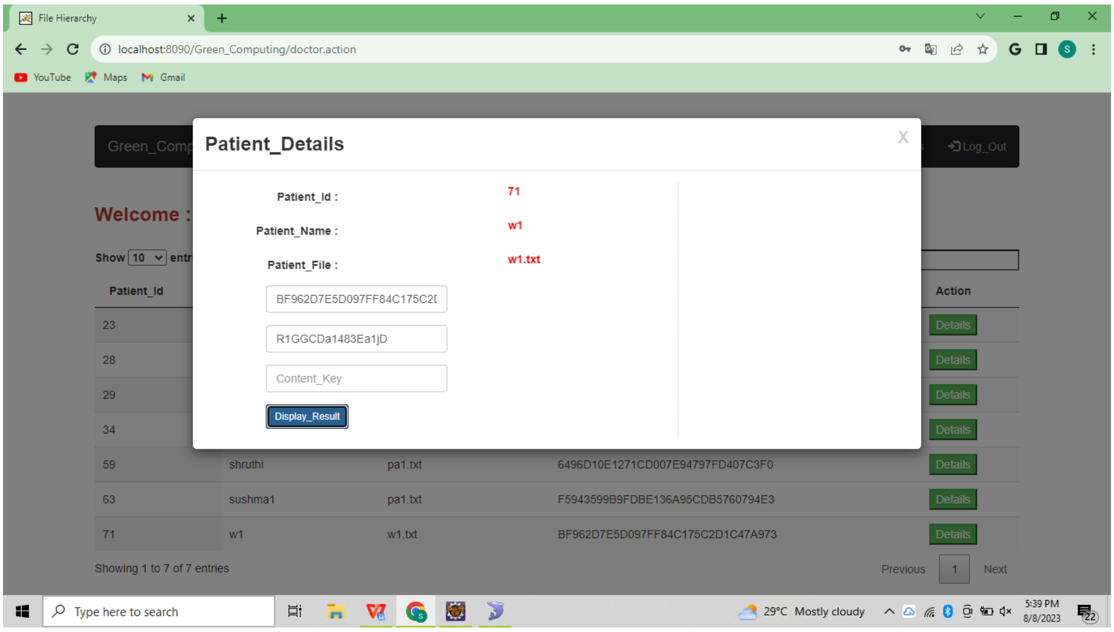
Show 10 entries

Search:

Patient_Id	Patient_Name	Patient_Record	Public_Key	Action
23	m1	m1.txt	53260A762D79E0AF6A66804ED8B22FBD	Details
28	arvind	arvind.txt	316A87D72D60A2BD8CA0CABB3C8BB0E4	Details
29	ps1	ps1.txt	3AB07034806D83623EA6A8DF44B274DA	Details
34	user1	user1.txt	B3BDF2D16C5D85B7D427E65ADEE6DDC8	Details
59	shruthi	pa1.txt	6496D10E1271CD007E94797FD407C3F0	Details
63	sushma1	pa1.txt	F5943599B9FDBE136A95CDB5760794E3	Details
71	w1	w1.txt	BF962D7E5D097FF84C175C2D1C47A973	Details

Showing 1 to 7 of 7 entries

✓ By using user authorization, this interface enables authorized users to extract information.



Patient_Details

Patient_Id : 71

Patient_Name : w1

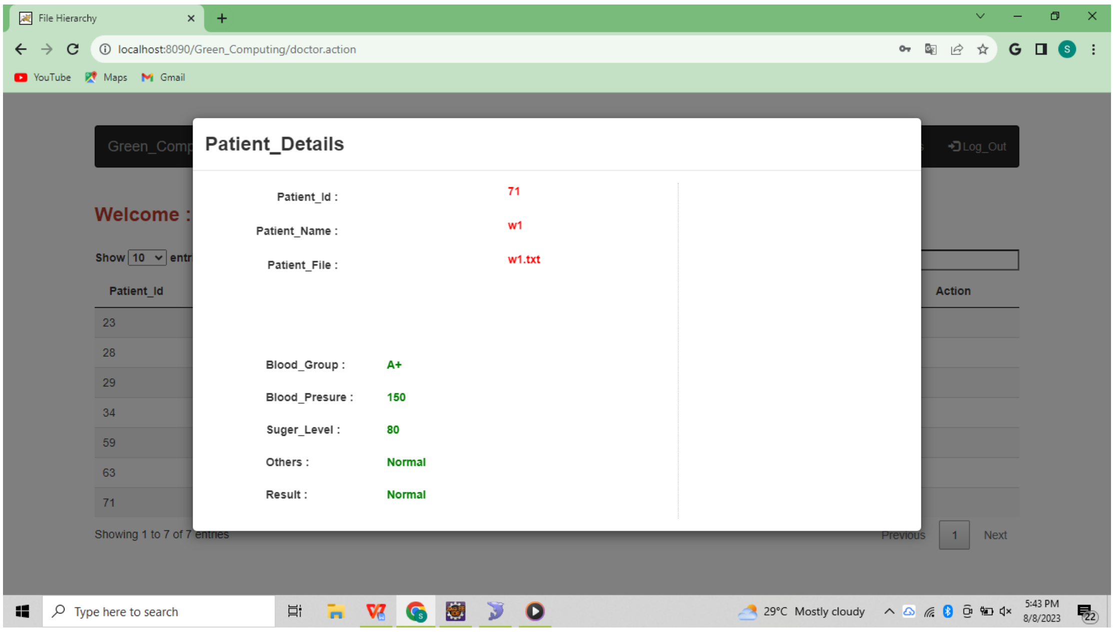
Patient_File : w1.txt

BF962D7E5D097FF84C175C2I

R1GGCDa1483Ea1jD

Content_Key

✓ The system asks the user to enter the content key after successfully verifying the public key and secret key in order to produce the desired output.



Patient_Details

Patient_Id : 71
Patient_Name : w1
Patient_File : w1.txt

Blood_Group : A+
Blood_Presure : 150
Suger_Level : 80
Others : Normal
Result : Normal

✓ If the key is determined to be correct after checking the public, secret, and content keys, the outcome will be shown.

CONCLUSION

In this research, we looked into how to maintain privacy while sharing enormous amounts of medical data in cloudlets and remote clouds. Our team has created a system that forbids users from sending information to a remote cloud, placing a higher priority on safe data collecting and minimal communication costs. Users can transfer data to a cloudlet, though, which creates a problem for data sharing.

We have put two important initiatives into place to deal with this problem. To begin with, we have used wearable technology to gather user data and cloudlet techniques to assure the safe transmission of that data. To evaluate whether data should be shared within the cloudlet, we have also created a trust model to gauge user trust levels.

In order to assure data privacy and improve transmission efficiency, we have also partitioned and encrypted the data stored in the remote cloud in several ways. Finally, to secure the entire system, we have suggested a collaborative IDS based on cloudlet mesh.
With the help of our system, people may ask questions of doctors online and get responses in return.

REFERENCE

1. Chen, M.,et al. (2017). "Privacy Protection and Intrusion Avoidance for Cloudlet- based Medical Data Sharing." IEEE Transactions on Cloud Computing.
2. Mitchell, R., & Chen, I.-R. (2015). "Behavior Rule Specification-based Intrusion Detection for Safety Critical Medical Cyber Physical Systems." IEEE Transactions on Dependable and Secure Computing, 12(1), 16-30.

3. Shi, Y., Abhilash, S., & Hwang, K. (2015). "Cloudlet Mesh for Securing Mobile Clouds from Intrusions and Network Attacks." In The Third IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (Mobile Cloud 2015).
4. Tadapaneni, N. R. (2017). "Different Types of Cloud Service Models." Available at SSRN 3614630.
5. Quwaider, M., & Jararweh, Y. (2015). "Cloudlet-based Efficient Data Collection in Wireless Body Area Networks." Simulation Modelling Practice and Theory, 50, 57-71.
6. Hossain, M. S. (2015). "Cloud-supported Cyber-Physical Localization Framework for Patients Monitoring."
7. Tadapaneni, N. R. (2018). "Cloud Computing: Opportunities and Challenges." International Journal of Technical Research and Applications.
8. Mohamed, H., Adil, L., Saida, T., & Hicham, M. (2013). "A Collaborative Intrusion Detection and Prevention System in Cloud Computing." In AFRICON, IEEE.
9. Zhang, R., & Liu, L. (2010). "Security Models and Requirements for Healthcare Application Clouds." In Cloud Computing (CLOUD), 2010 IEEE.
10. Hung, K., Zhang, Y., & Tai, B. (2004). "Wearable Medical Devices for Telehome Healthcare." In Engineering in Medicine and Biology Society, 2004. IEMBS'04. 26th Annual International Conference of the IEEE (Vol. 2). IEEE.
11. Guiwu, W. Y. (2018, June). "Research on Genetic Algorithm for Resource Scheduling in Cloud Computing Based on User Satisfaction." In 5th International Conference on Electrical & Electronics Engineering and Computer Science (ICEEECS 2018) (Vol. 5).
12. Patel, A., & Tiwari, P. (2018). "Cloud Computing Security, Privacy Improvements Using Virtualized High Trust Zone." International Journal of Modern Trends in Engineering and Science, 3(12).