

SECURITY FEATURES OF CLOUD COMPUTING

Aliena Fatima, Mrs. M.Anusha

¹B.tech Student, Department Of Electronics and Computer Engineering, J.B Institute of Engineering and Technology

²Assistant Professor, Department Of Electronics and Computer Engineering, J.B Institute of Engineering and Technology

Abstract: Cloud Computing is increasingly becoming popular as many enterprise applications and data are moving into cloud platforms. However, a major barrier for cloud adoption is lack of security. In this paper, we take a holistic view of cloud computing security – spanning across the possible issues and vulnerabilities connected with software platform, identity management and access control, data integrity, confidentiality and privacy, physical and process security aspects, and legal compliance in cloud. We present our findings from the points of view of a cloud service provider, cloud consumer, and third-party authorities such as Govt. We also discuss important research directions in cloud security in areas such as Trusted Computing, Information Centric Security and Privacy Preserving Models. Finally, we sketch a set of steps that can be used, at a high level, to assess security preparedness for a business application to be migrated to cloud.

INTRODUCTION

With the rapid development of cloud computing, big data and public cloud services have been widely used. The user can store his data in the cloud service. Although cloud computing brings great convenience to enterprises and users, the cloud computing security has always been a major hazard. For users, it is necessary to take full advantage of cloud storage service, and also to ensure data privacy. Therefore, we need to develop an effective access control solution. Since the traditional access control strategy cannot effectively solve the security problems that exist in data sharing. Data security issues brought by data sharing have seriously hindered the development of cloud computing, various solutions to achieve encryption and decryption of data sharing have been proposed. In 2007, Bethencourt et al. first proposed the ciphertext policy attribute-based encryption (CP-ABE). However, this scheme does not consider the revocation of access permissions. In 2011, Hur et al. put forward a fine-grained revocation scheme but it can easily cause key escrow issue. Lewko et al. used multi authority ABE (MA-ABE) to solve key escrow issue. But the access policy is not flexible. Li et al presented data sharing scheme based on systemic attribute encryption, which endows different users' different access rights. But it is not efficient from the complexity and efficiency. In 2014, Chen et al. proposed Key-Aggregate Encryption algorithm, effectively shortening the length of the ciphertext and the key, but only for the situation where the data owner knows the user's identity. These schemes above only focus on one aspect of the research, and do not have a strict uniform standards either. In this paper, we present a more systematic, flexible and efficient access control scheme.

LITERATURE SURVEY

Cloud Computing: Secure, Scalable, and Fine-grained Data Access Control

An evolving computer paradigm, cloud computing provides computing infrastructure resources as Internet services. As promising as it is, this paradigm introduces numerous new data security and access control concerns when users share sensitive data on cloud servers, which are not trusted by data owners. Existing solutions employ cryptography to protect sensitive user data from untrusted servers by releasing data decryption keys to authorized users. These methods do not scale well because they need the data owner to compute heavily for key distribution and data management when finegrained data access control is sought. Access control still struggles to balance fine-grainedness, scalability, and data secrecy. This paper addresses this difficult open issue by defining and enforcing data attribute-based access policies and allowing the data owner to delegate most of the computation tasks involved in finegrained data access control to untrusted cloud servers without disclosing the dataset. We exploit and uniquely combine attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption to accomplish this aim. User access privilege secrecy and secret key accountability are also important in our strategy. Our system is efficient and safe under current security models, according to extensive investigation.

Policy-based encryption of bounded ciphertext

Using ciphertext policy attribute-based encryption, a user's private key is associated with a set of attributes, and an encrypted ciphertext specifies an access policy over attributes. Users may decrypt if their characteristics match the ciphertext's policy. We provide the first ciphertext policy attribute-based encryption system with a number theoretic security proof and sophisticated access mechanisms. Previous CP-ABE systems supported only restricted access structures or simply offered generic group model security proofs. Our approach supports access structures with restricted size access trees with threshold gates as nodes. The access tree size limit is specified during system setup. We use the Decisional Bilinear DiffieHellman assumption for our security proof.

Attribute-based encryption enables secure sharing of personal health data in cloud computing.

An growing patient-centric approach of health information interchange, personal health records (PHR) are typically outsourced to cloud companies. Many privacy issues exist because third-party servers might disclose sensitive health information to unauthorized parties. To provide patients control over their PHRs, encrypting them before outsourcing appears promising. However, privacy hazards, key management scalability, flexible access, and efficient user revocation remain the biggest obstacles to fine-grained, cryptographically enforced data access control. This study introduces a patient-centric architecture and data access control techniques for semi-trusted server PHRs. We encrypt each patient's PHR file using attribute-based encryption (ABE) for fine-grained and scalable data access control. Unlike past safe data outsourcing operations, we concentrate on various data owners and separate PHR system users into several security domains, reducing critical administrative complexity for owners and users. Using multi-authority ABE ensures patient privacy. Our system

offers dynamic access policy or file attribute update, on-demand user/attribute revocation, and emergency break-glass access.

Key-Aggregate Cryptosystem for Cloud Storage Scalable Data Sharing

Sharing data is crucial in cloud storage. This article explains how to safely, effectively, and flexibly transfer cloud storage data. We provide novel public-key cryptosystems that generate constant-size ciphertexts enabling efficient decryption rights delegation for any collection of ciphertexts. Aggregating any group of secret keys into a single key with the power of all the keys is innovative. The secret key holder may release a constant-size aggregate key for flexible cloud storage ciphertext set options, but encrypted data outside the set remain private. Send this little aggregate key to others or put it on a smart card with limited safe storage. Our approaches are formalized for security analysis in the standard model. Other applications of our techniques are also described. Our techniques provide the first public-key patient-controlled encryption with flexible hierarchy.

Signatures without anonymity revocation using hidden attributes

The recent improvements in attribute-based cryptosystem motivated us to propose concealed attribute-based signature. You may sign messages with any subset of your attributes from an attribute center using this method. This view holds that a signature attests to the signer's traits, not their identity. Users cannot fake signatures with unissued characteristics. The signer stays anonymous without risk of revocation among all users having the signature's qualities. After formalizing the security paradigm, we propose two pairing-based hidden attribute signatures. The first design supports a vast universe of characteristics and depends on the random oracle assumption for security, which the second architecture removes. Under the computational Diffie–Hellman assumption, both constructs are safe. This study introduced concealed attribute-based signature. Also recommended and established were security definitions and models. Hidden attribute-based signatures are unforgeable and anonymous. Unforgeability means that a person lacking certain traits cannot sign with unachievable attributes. The signer may construct a signature using part of his qualities and remain anonymous to all users with the same attributes. We also presented two hidden attribute-based signature constructions in this work. The first structure allows a vast universe of characteristics and depends on the random oracle assumption for security, whereas the second construction does not. The basic computational Diffie–Hellman assumption secures both constructs.

ANALYSIS

It includes a set of use cases that describe all the interactions the users will have with the software. In addition to use cases, the SRS also contains non-functional requirements. Nonfunctional requirements are requirements which impose constraints on the design or implementation (such as performance engineering requirements, quality standards, or design constraints). System requirements specification: A structured collection of information that embodies the requirements of a system. A business analyst, sometimes titled system analyst, is responsible for analyzing the business needs of their clients and stakeholders to help identify business problems and propose solutions. Within the systems development lifecycle domain, the BA typically performs a liaison

function between the business side of an enterprise and the 20 information technology department or external service providers. Projects are subject to three sorts of requirements:

Business requirements describe in business terms what must be delivered or accomplished to provide value.

Product requirements describe properties of a system or product (which could be one of several ways to accomplish a set of business requirements.) Process requirements describe activities performed by the developing organization.

DESIGN

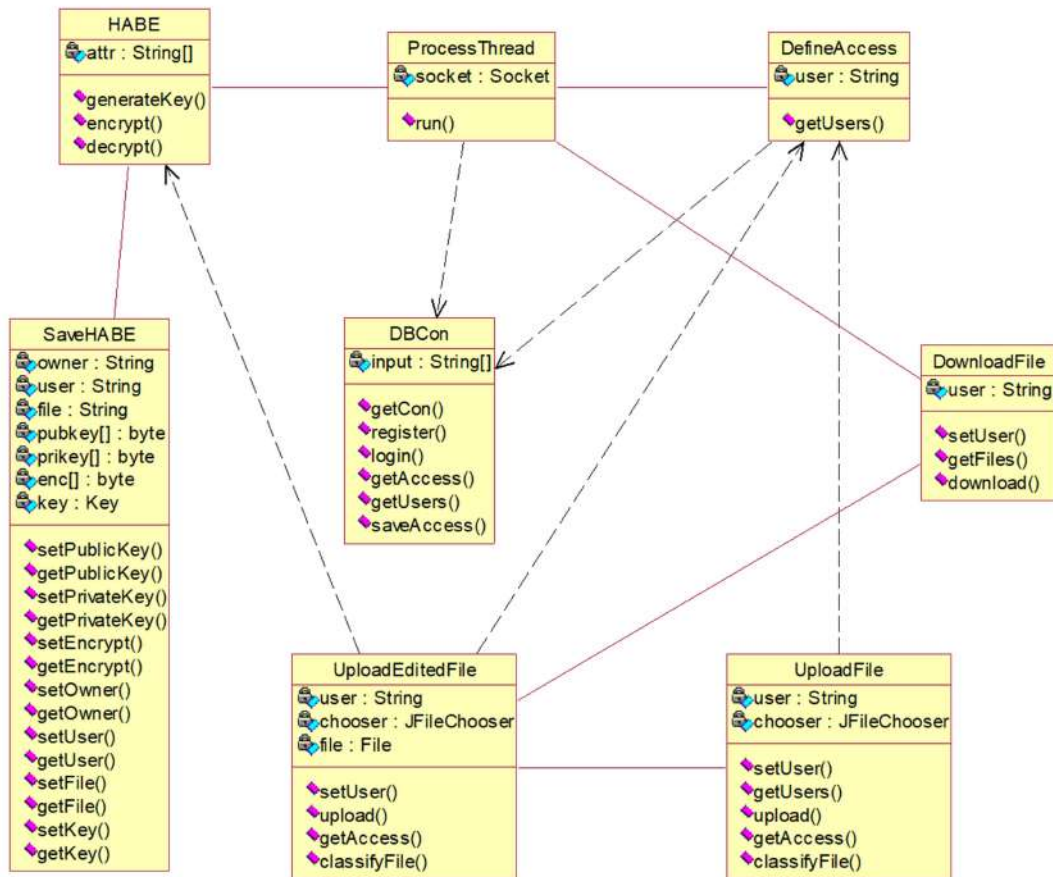
4.1 Introduction

4.2 UML diagrams

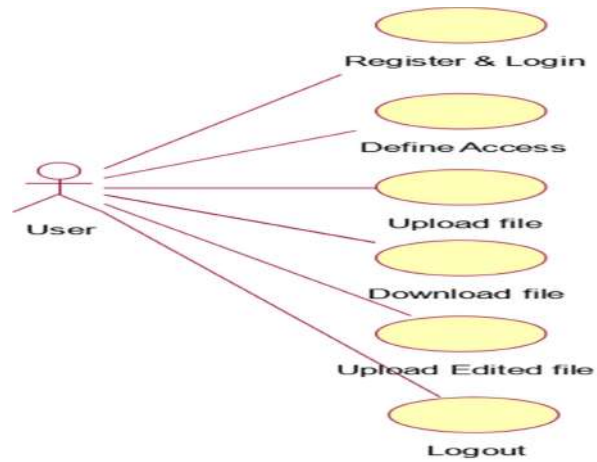
The Unified Modeling Language allows the software engineer to express an analysis model using the modeling notation that is governed by a set of syntactic semantic and pragmatic rules. A UML system is represented using five different views that describe the system from distinctly different perspective. Each view is defined by a set of diagram, which is as follows:

DIAGRAMS

Class Diagram

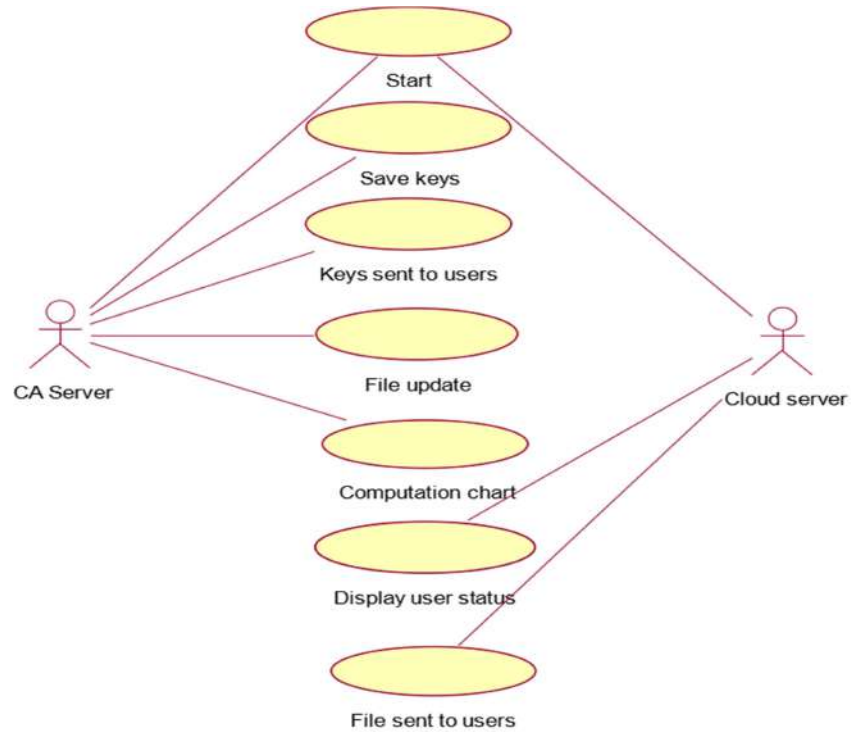


Use Case Diagram

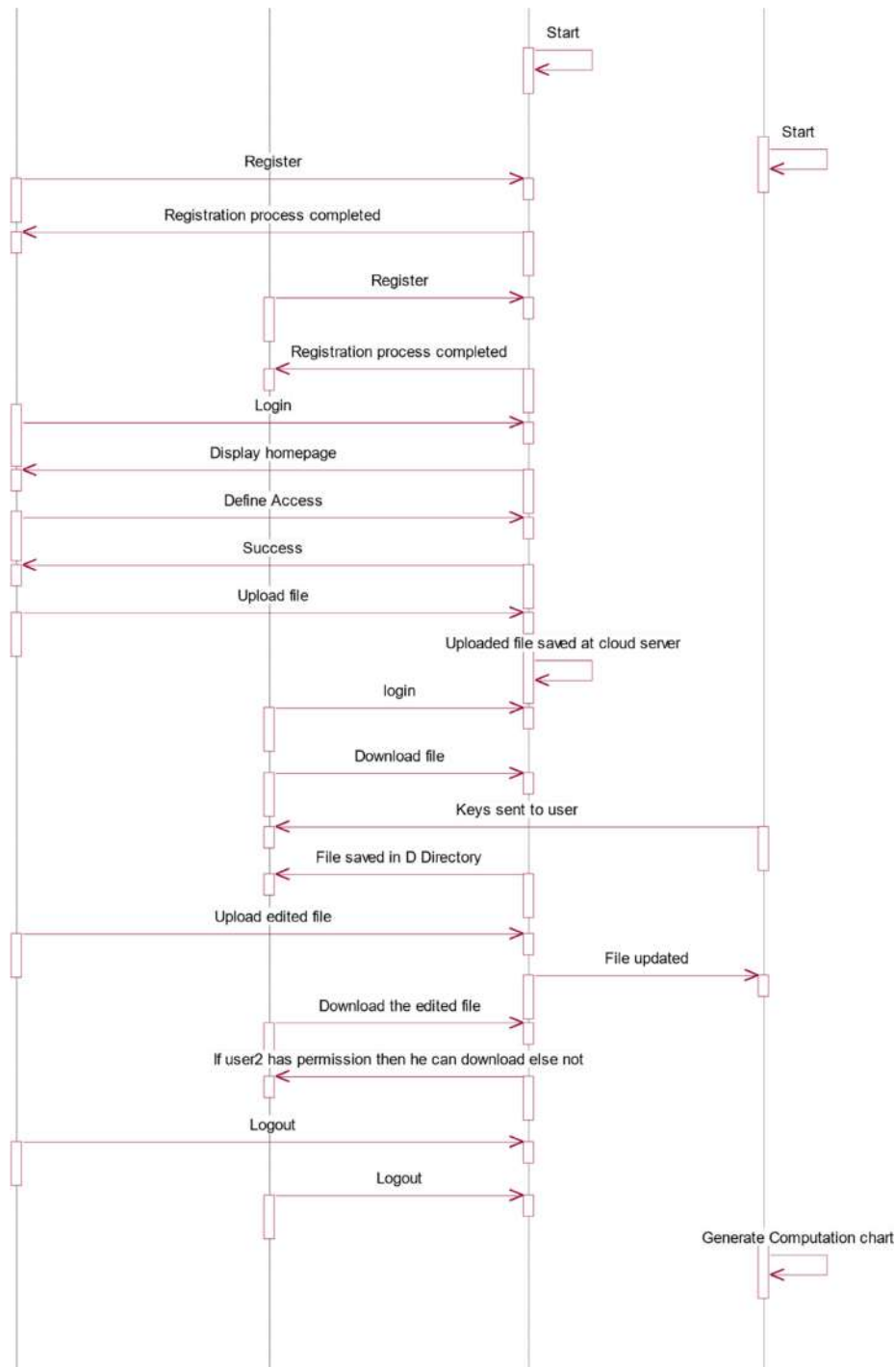


Use Case Diagram for User

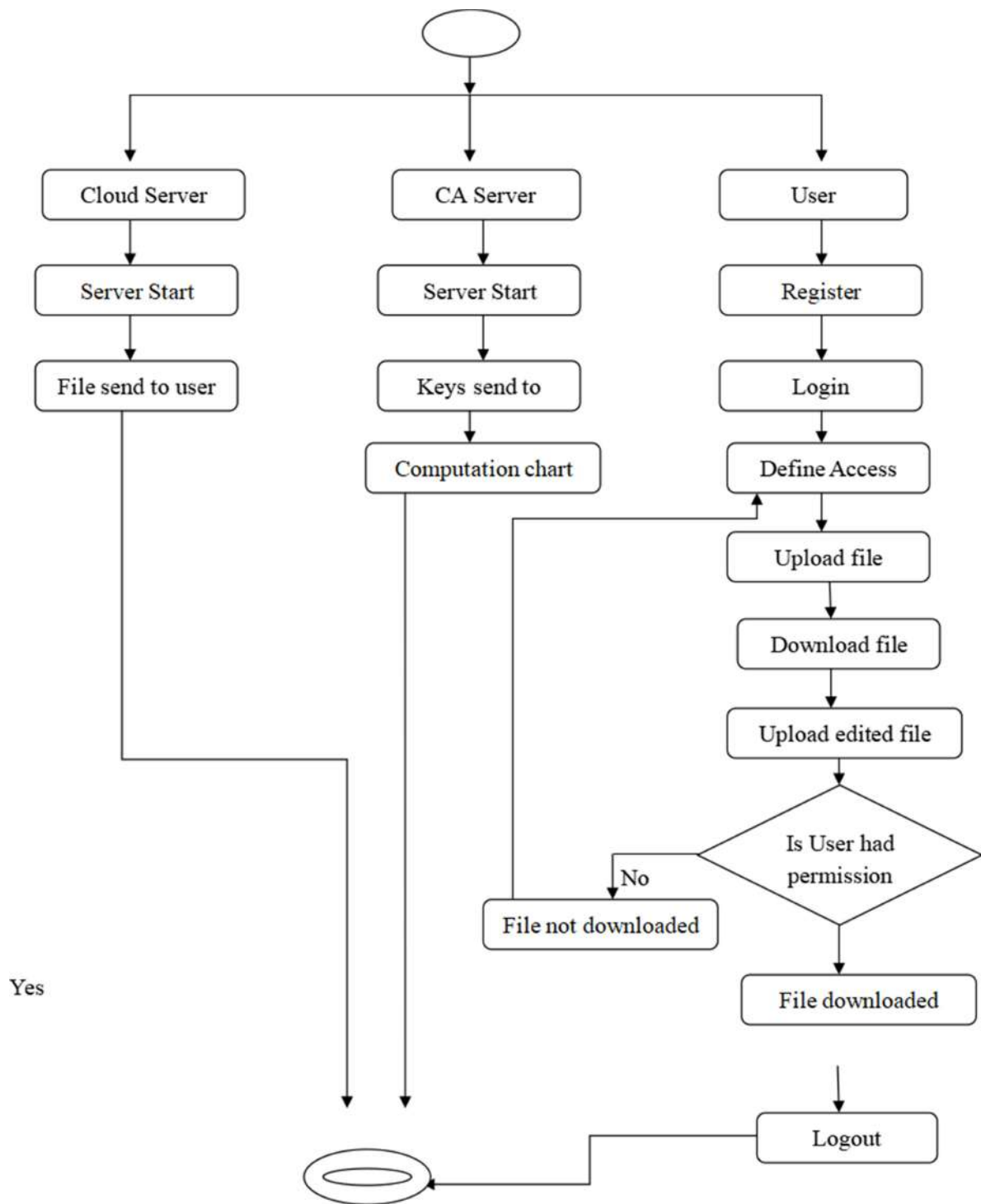
Use Case Diagram for Server



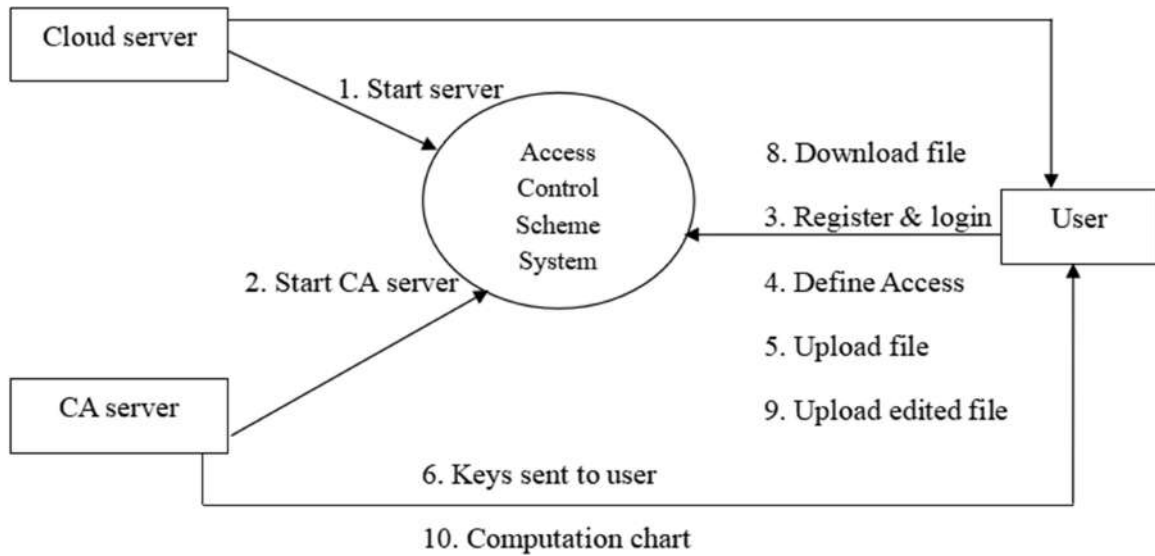
Sequence Diagram:



Activity Diagram:



Data Flow Diagram:



IMPLEMENTATION AND RESULTS

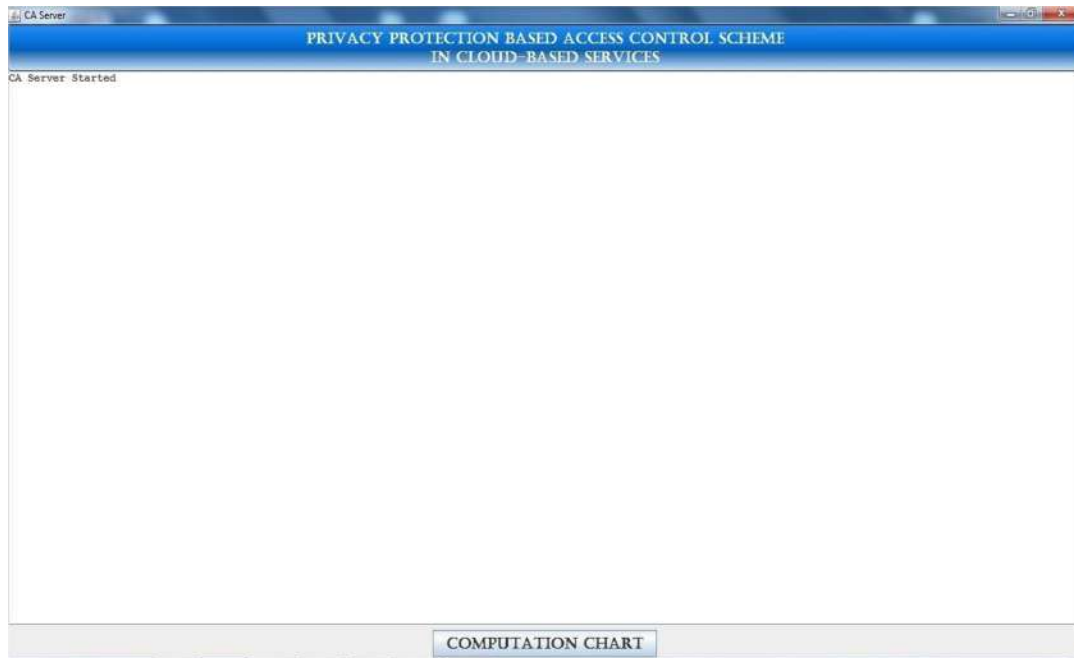
5.1 Introduction

This chapter tells us about the implementation part of the website. This section deals with the brief introduction about the important functions used to create the security features of cloud computing. It consists of various source codes used in building this web page. Also lists out the outputs of each section which makes it clear about the different options available to complete the quiz successfully.

Output Screens



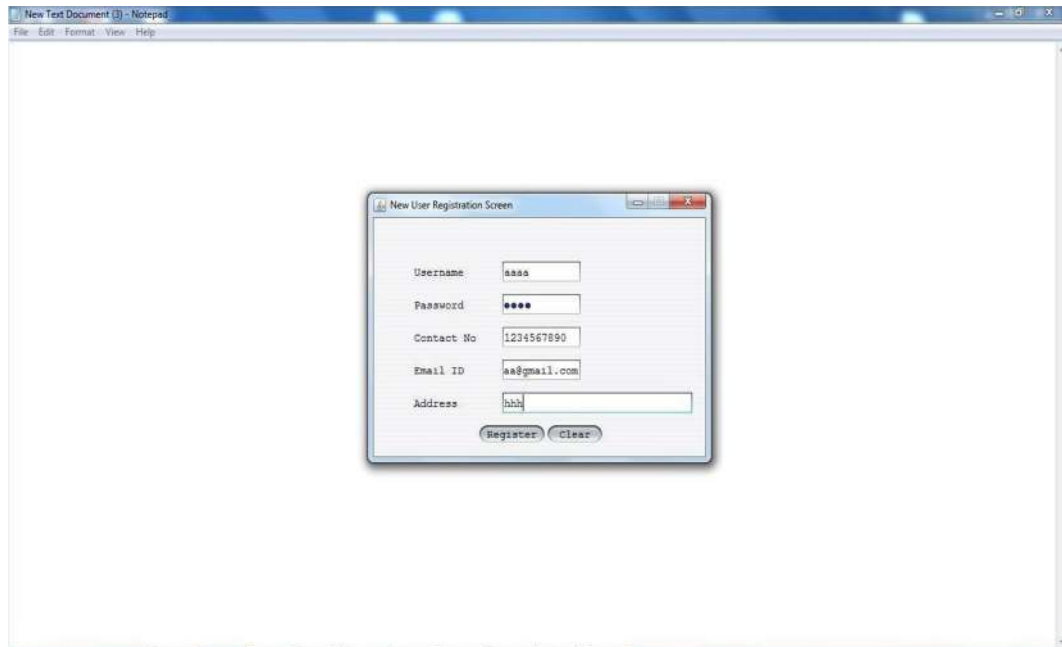
Cloud Server



CA Server



User Application Web Screen



New Text Document (3) - Notepad

File Edit Format View Help

New User Registration Screen

Username:

Password:

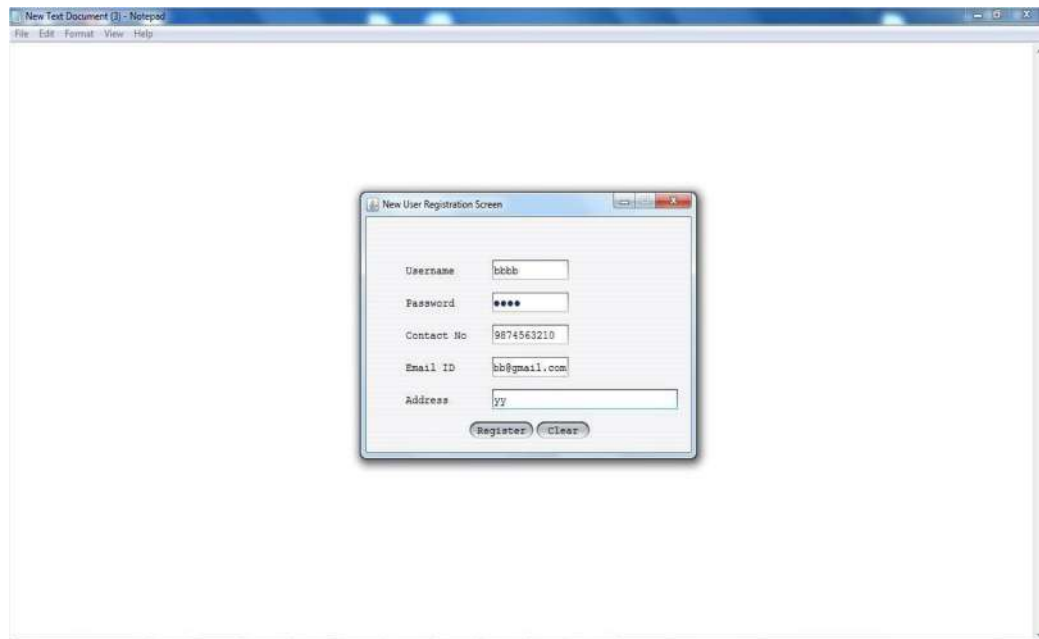
Contact No:

Email ID:

Address:

Register Clear

Click on new user to register the user



New Text Document (3) - Notepad

File Edit Format View Help

New User Registration Screen

Username:

Password:

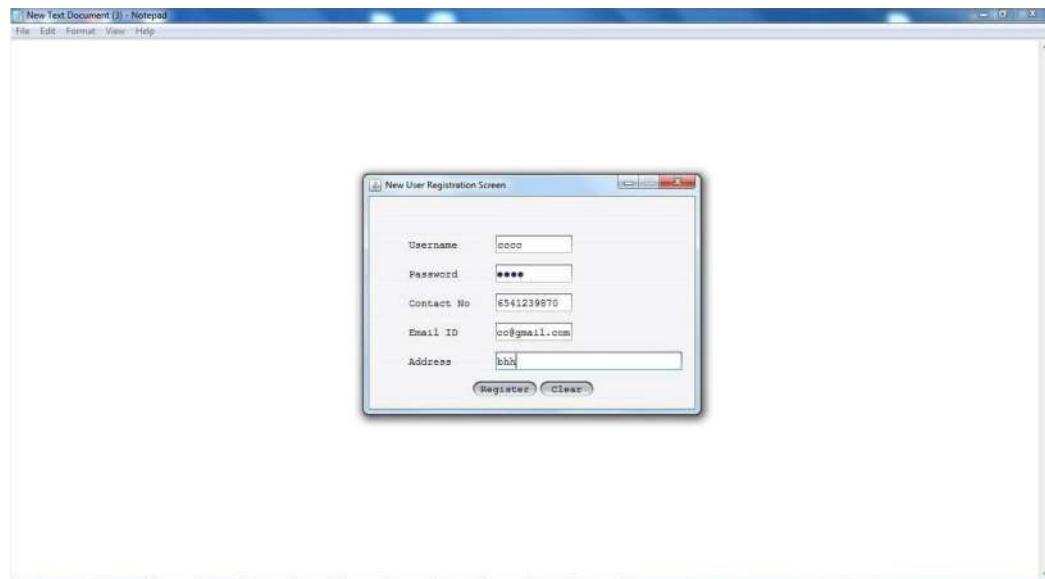
Contact No:

Email ID:

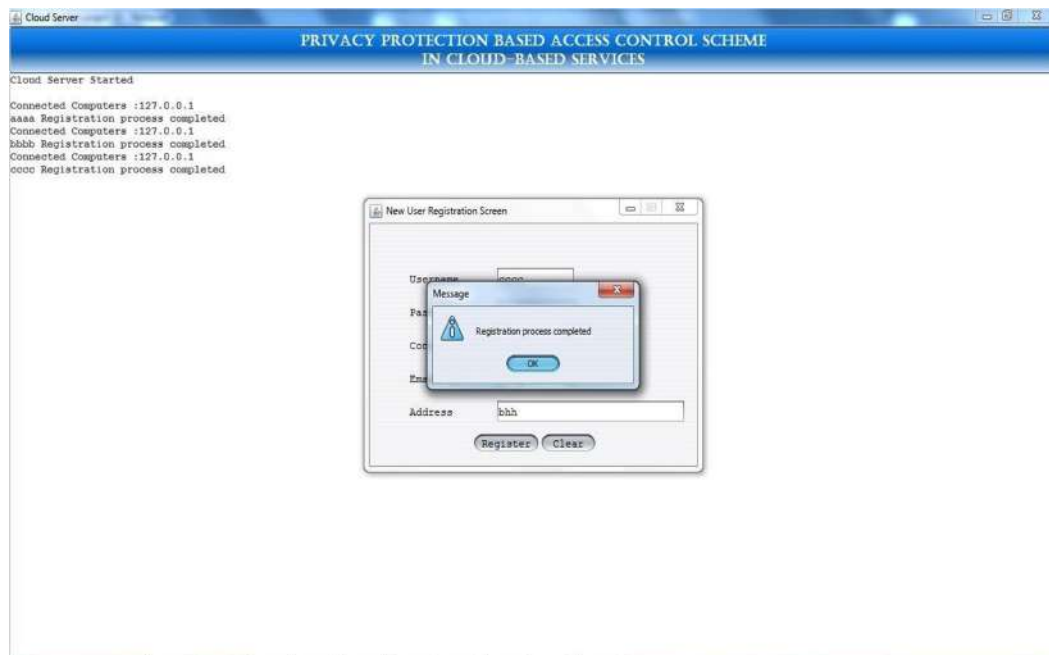
Address:

Register Clear

Registering another user



Registering another user



After successfully registering the users



Login as registered user



User Home screen

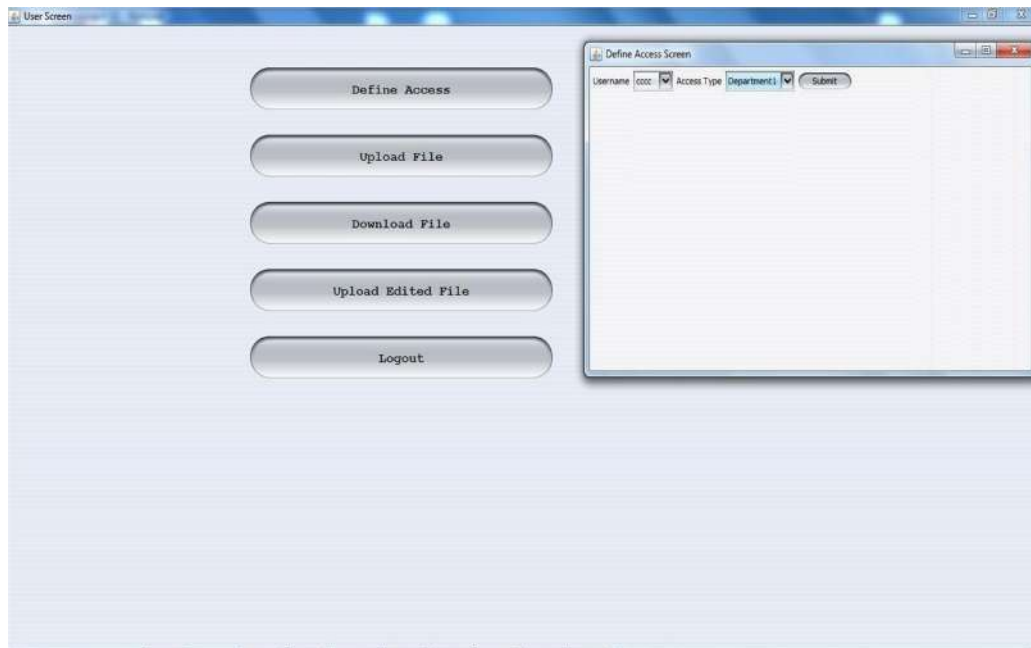
Define Access:

(Here while defining access, 2 types of users will there. Personnel domain (PSD) and public domain (PUD).

PSD users will have both read and write operation whereas the PUD users will have only the read operations. In our application family, friend and colleague will be considered as PSD and department1, 2, 3, 4 will be considered as PUD) Here for the user (bbbb) giving the access type as PSD:



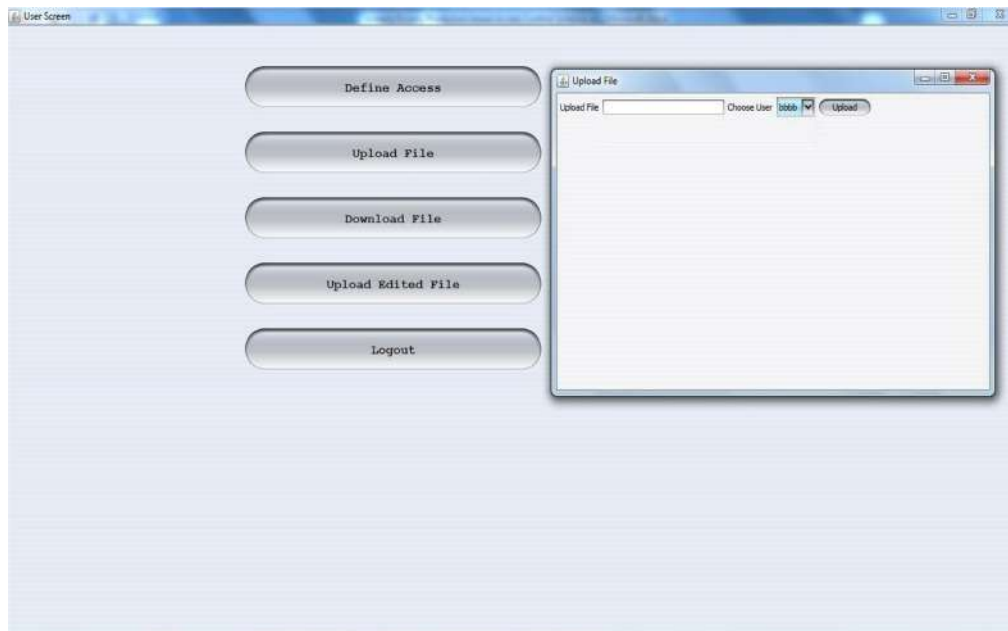
Define Access



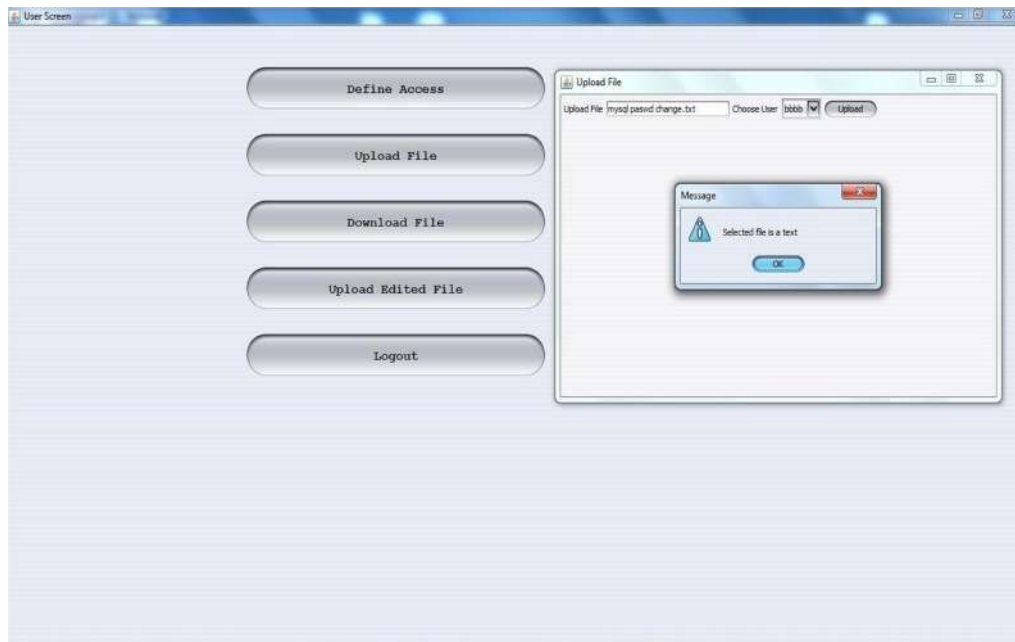
Giving (cccc) access type as PUD



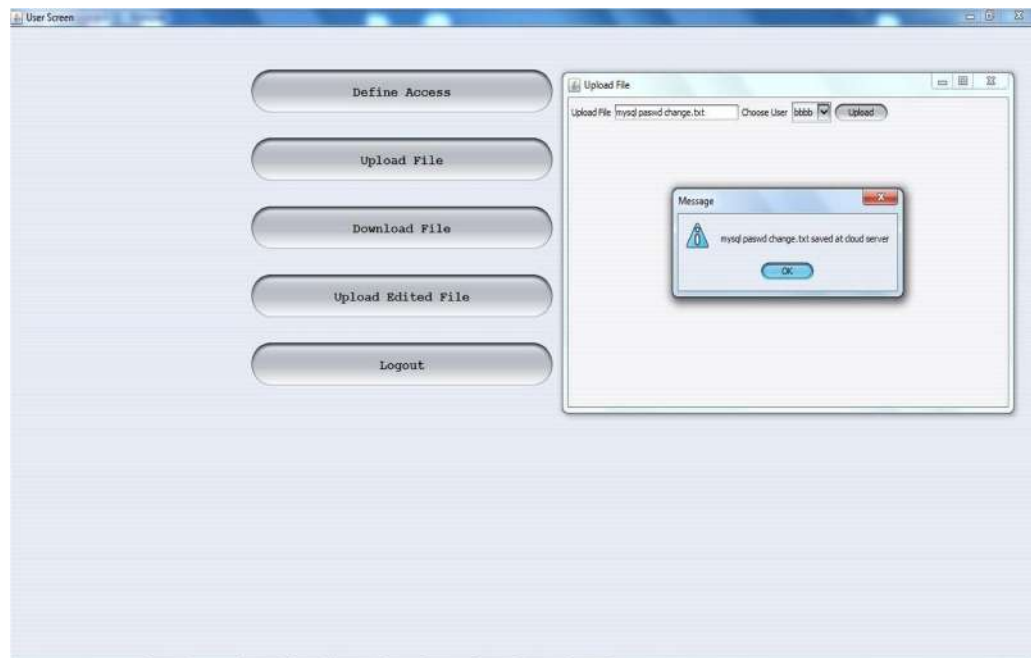
After successfully giving access permission



User upload file screen



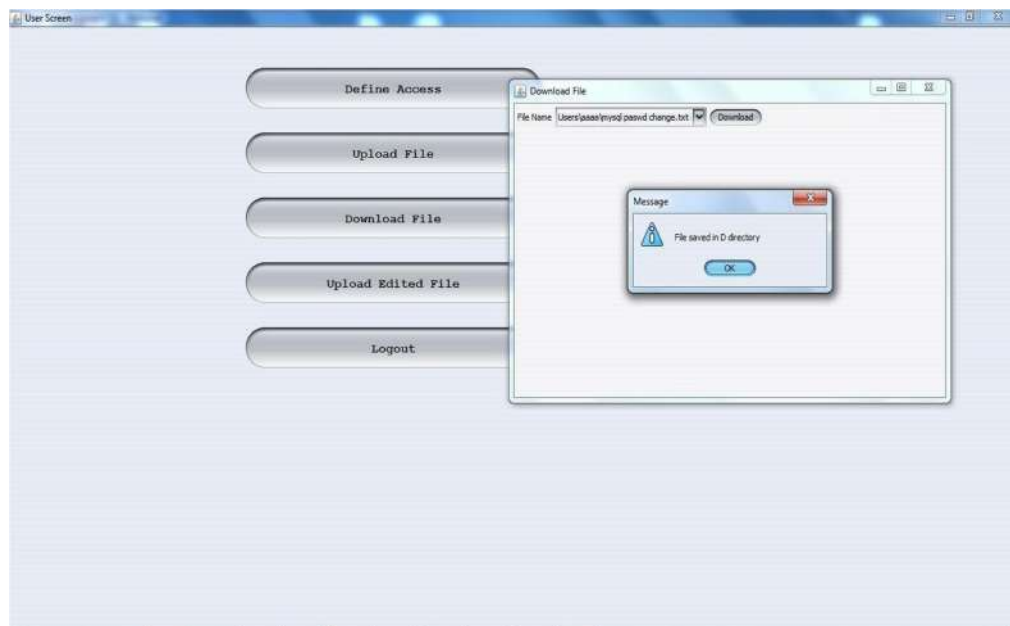
Select the user, and select a file to be uploaded to cloud:



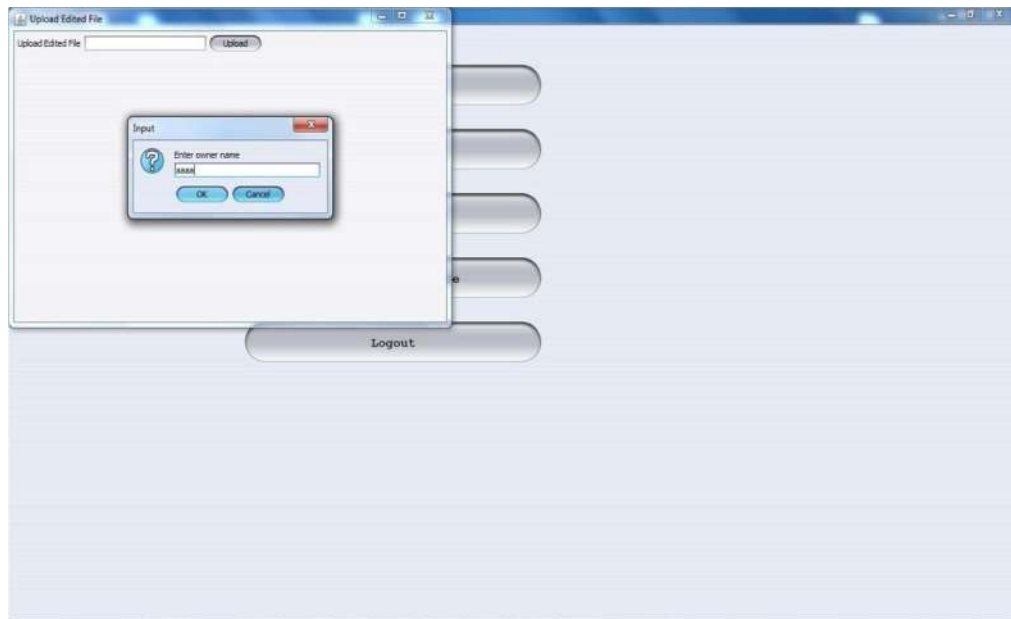
After uploading the file to cloud



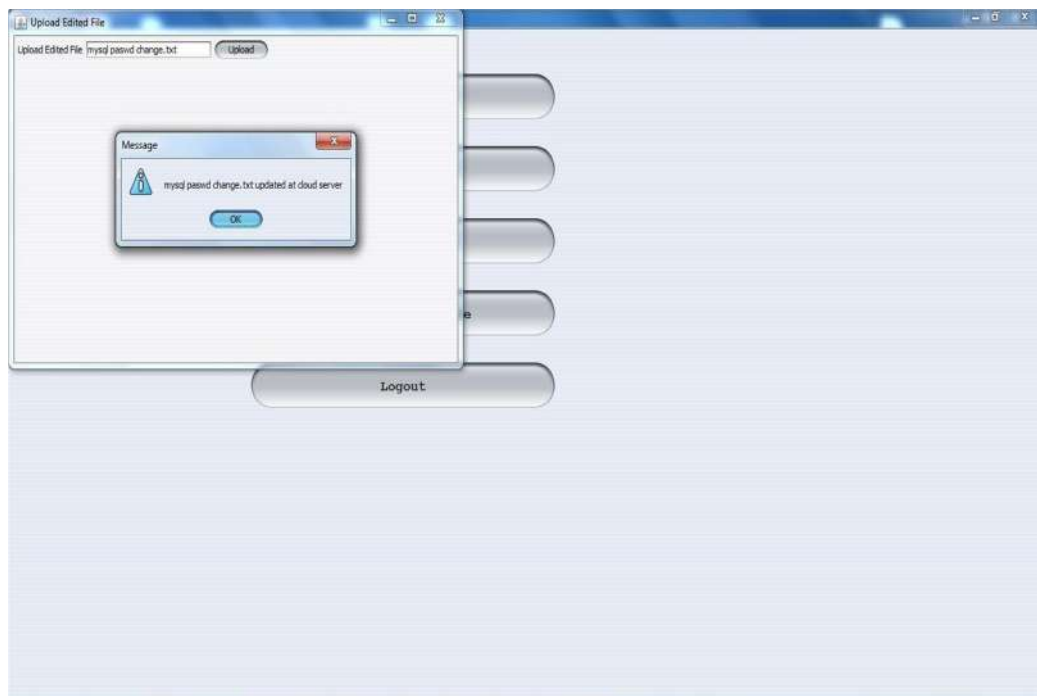
Login as PSD User



User downloading the file

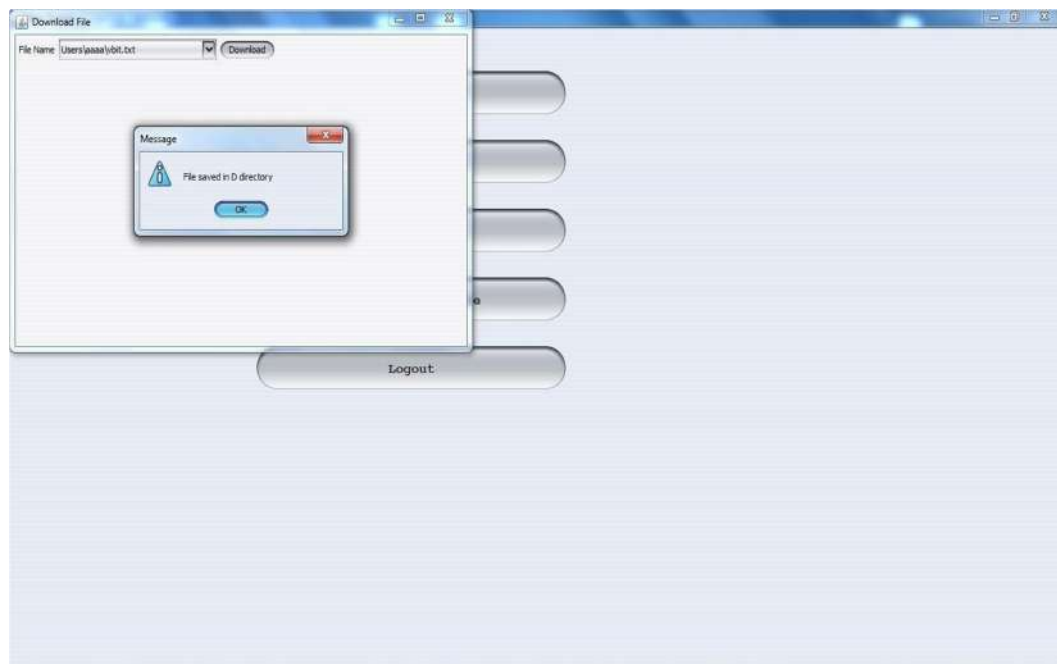


User uploading the edited file

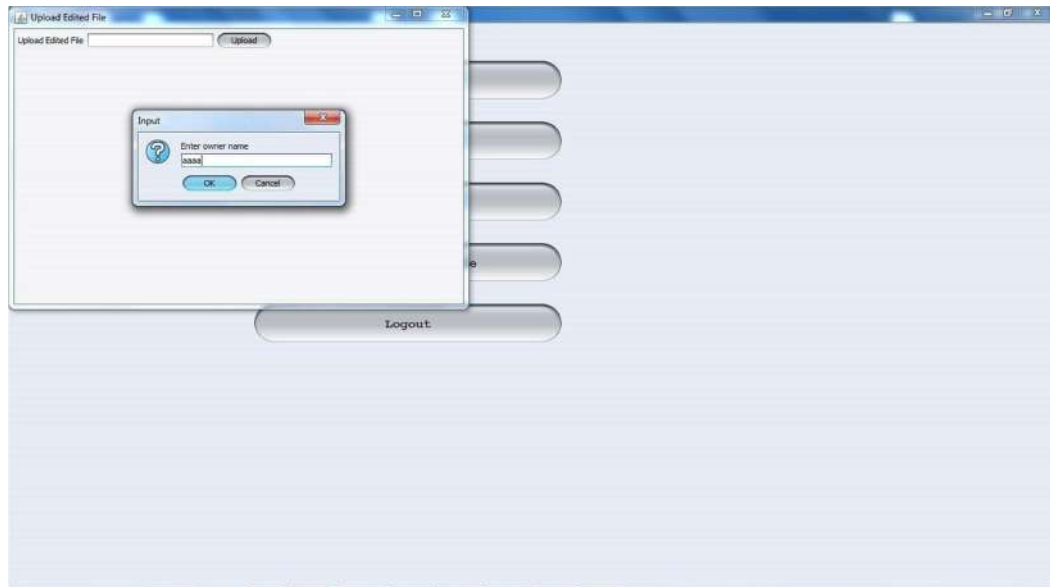




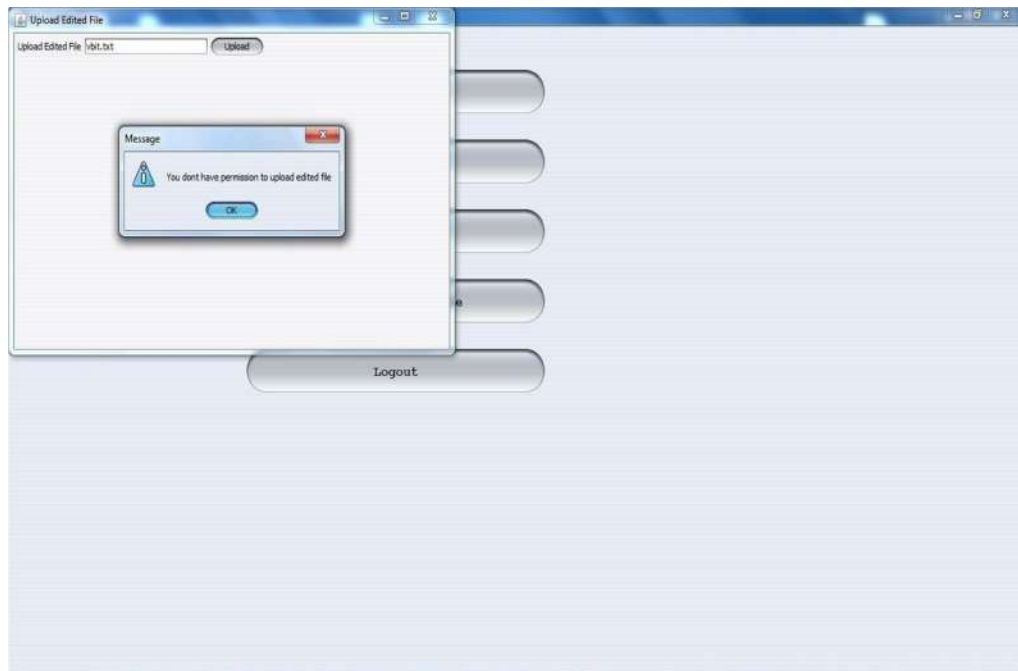
Login as a PUD User



Downloading the file

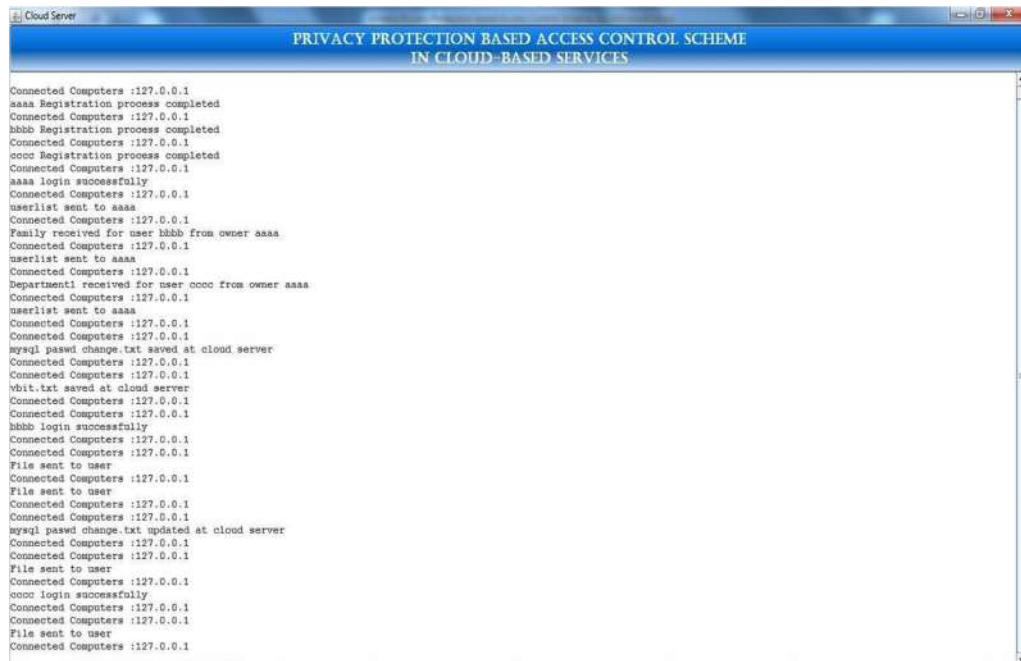


Upload the edited file but it won't be reflected in cloud





CA Server



Cloud Server

CONCLUSION

Conclusion:

In this paper, we propose access control system (PS-ACS), which is privilege separation based on privacy protection. Through the analysis of cloud environment and the characteristics of the user, we divide the users into personal domain (PSD) and public domain(PUD) logically. In the PSD, the KAE algorithm is applied to implement users read access permissions and greatly improved efficiency. The IABS scheme is employed to achieve the write permissions and the separation of read and write permissions to protect the privacy of the user's identity. In the PUD, we use the HABE scheme to avoid the issues of single point of failure and to achieve data sharing. Furthermore, the paper analyzes the scheme from security and efficiency, and the simulation results are given. By comparing with the MAH-ABE scheme, the proposed scheme shows the feasibility and superiority to protect the privacy of data in cloud-based services.

Future Scope:

While a multi-cloud approach can provide many benefits, it also introduces challenges from a security perspective. One major issue is the risk of data silos, as data may be spread across multiple platforms and locations. This can make it difficult to capture and analyze incident data, leading to potential gaps in security and risk management. To address these challenges, organizations require a cohesive approach to managing security across multiple platforms. This may involve investing in security tools that provide cross-cloud support so that security teams can seamlessly investigate incident data – regardless of where it resides.

The above-mentioned points are the enhancements that can be done to increase the applicability and usage of this project.

REFERENCES:

- [1] S. Yu, C. Wang, K. Ren, “Achieving secure, scalable, and fine-grained data access control in cloud computing,” Proc. IEEE INFOCOM, pp. 1-9, 2010.
- [2] J. Bethencourt, A. Sahai, B. Waters, “Ciphertext-policy attribute-based encryption,” Proc. Security and Privacy, pp. 321-334, 2007.
- [3] J. Hur, D.K. Noh, “Attribute-based access control with efficient revocation in data outsourcing systems,” IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 7 pp. 1214-1221, 2011.
- [4] J A. Lewko, B. Waters, “Decentralizing attribute-Based encryption,” Proc. Advances in CryptologyEUROCRYPT, pp. 568-588, 2011.
- [5] M. Li, S. Yu, Y. Zheng, “Scalable and secure sharing of personal health records in cloud computing using attribute-Based Encryption,” IEEE Transactions on Parallel and Distributed System, vol. 24, no. 1, pp. 131- 143, 2013.
- [6] C.K. Chu, S.S.M. Chow, W.G. Tzeng, “Key-aggregate cryptosystem for scalable data sharing in cloud storage,” IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp.468-477, 2014.
- [7] J. Li, K. Kim, “Hidden attribute-based signatures without anonymity revocation,” Information



Sciences, vol. 180, no. 9, pp. 1681-1689, 2010.

- [8] H.K. Maji, M. Prabhakaran, M. Rosulek, "Attribute-Based Signatures," Proc. Topics in Cryptology - CTRSA, pp. 376-392, 2011.
- [9] S. Kumar, S. Agrawal, S. Balaraman, "Attribute based signatures for bounded multi-level threshold circuits," Proc. Public Key Infrastructures, Services and Applications, pp. 141-154, 2011