Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Cloud-Based Services Use Access Control with Privacy Protection

ZebaFarheen Kazi[1] , Sujata Gaikwad[2]

[1]M.techStudent, Department of Computer Science and Engineering,TPCT's College of Engineering Osmanabad,Maharashtra,India, E-MAIL: kazizebafarheen22@gmail.com

[2]Head of Department, Department of Computer Science and Engineering,TPCT's College of Engineering Osmanabad,Maharashtra,India, E-MAIL:sujatagaikwad414@gmail.com

Abstract-Cloud-based services are a prominent topic now that computer technology is advancing so quickly. Users of cloud-based services experience convenience as well as several security risks. Therefore, it is crucial to research access control methods to safeguard users' privacy in cloud environments. In this research, we describe a privilege-based access control system for protecting privacy (PS-ACS). The users are conceptually separated into personal domain (PSD) and public domain (PUD) in the PS-ACS method. We gave users read and write access privileges in the PSD, accordingly. The read access permission is implemented using the Key-Aggregate Encryption (KAE), which increases access effectiveness. By utilising an Improved Attribute-based Signature (IABS) that can determine the users' write access, a high level of patient privacy is simultaneously guaranteed. Hierarchical attribute-based encryption (HABE) is used for PUD users in order to get beyond the problems of single point of failure and convoluted key distribution. The results of the function and performance tests demonstrate the PS-ACS scheme's ability to secure user privacy in cloud-based services.

Keyword :Public Domain(PUD),Private Domain (PRD), Hierarchical Attribute Based Encryption(HABE), Cipertext-policy Attribute Based Encryption(CP-ABE), Multi-Authority Attribute Based Encryption(MA-ABE).

I.INTRODUCTION

Cloud-based services are a hot topic now that computer technology is advancing so quickly. Users of cloud-based services experience convenience as well as several security risks. Therefore, it is crucial to research access control methods to safeguard users' privacy in cloud environments. In this research, we describe a privilege-based access control system for protecting privacy (PS-ACS). The users are conceptually separated into personal domain (PSD) and public domain (PUD) in the PS-ACS method. We gave users read and write access privileges in the PSD, accordingly. The read access permission is implemented using the Key-Aggregate Encryption (KAE), which increases access effectiveness. Utilizing an Improved Attribute-based Signature (IABS) that can determine the users' write access ensures a high level of patient privacy at the same time. To prevent problems with single points of failure and convoluted key distribution for PUD users, hierarchical attribute-based encryption (HABE) is used. The PS-ACS scheme was found to be capable of achieving privacy protection in cloud-based services by the results of function and performance testing.The PS-ACS scheme was found to be capable of achieving privacy protection in cloud-based services by the results of function and performance testing.Big data and public cloud services have become increasingly popular as a result of the quick growth of cloud computing. The user can utilise the cloud service to store his data. Cloud computing security has always been a significant risk, despite the fact that it offers businesses and customers a lot of ease. Users must maintain data privacy in addition to making the most of cloud storage services. Therefore, we must create a reliable access control system. Since the security issues with data sharing cannot be adequately solved by the conventional access control technique [1]. A number of techniques to achieve encryption and decryption of data sharing have been proposed. Data security challenges brought on by data sharing have substantially hampered the development of cloud computing.Users must maintain data privacy in addition to making the most of cloud storage services. Therefore, we must create a reliable access control system. Since the security issues with data sharing cannot be adequately solved by the conventional access control technique [1]. A number of techniques to achieve encryption and decryption of data sharing have been proposed. Data security challenges brought on by data sharing have substantially hampered the development of cloud computing. The ciphertext policy attribute-based encryption was first proposed by Bethencourt et al. in 2007 [2]. (CP-ABE). This plan, however, does not account for access permissions being revoked. Hur et al. [3] proposed a fine-grained revocation mechanism in 2011, however it is susceptible to key escrow issues. Key escrow issue was resolved by Lewko et al. [4] using multi authority ABE (MA-ABE). The access policy, however, is rigid. Li et al. presented a method for sharing data that is based on systemic attribute encryption and grants various users with varying levels of

access. However, despite its complexity and inefficiency. The length of the ciphertext and the key areeffectively reduced by the Key-Aggregate Encryption technique Chen et al. [6] developed in 2014, but only when the data owner is aware of the user's identity. These plans listed above do not adhere to stringent uniform standards and solely concentrate on one component of the research. In this article, we provide a better organised, adaptable, and effective access control system.

II.PROPOSED SYSTEM

• We put forth PSACS, a cutting-edge access control system that separates privileges based on privacy protection. The read access control method is implemented by the system using the Key-Aggregate Encryption (KAE) and Hierarchy Attribute-based Encryption (HABE) schemes in the PSD and PUD, respectively.

• The HABE scheme substantially decreases the workload of a single authority and safeguards user data privacy, while the KAE scheme significantly increases access efficiency.

•We use an Improved Attribute-based Signature (IABS) scheme to implement write access control in the PSD as opposed to the MAH-ABE technique, which ignores write access control. By doing this, the user can successfully edit the file and pass the cloud server's signature verification without having to reveal their identity.

III. MODULE DESCRIPTION

Our system model is shown in Fig. 1 by the following entities: Data owner, users in PSD and PUD, root authority CA, regional authority AA, and cloud service provider.

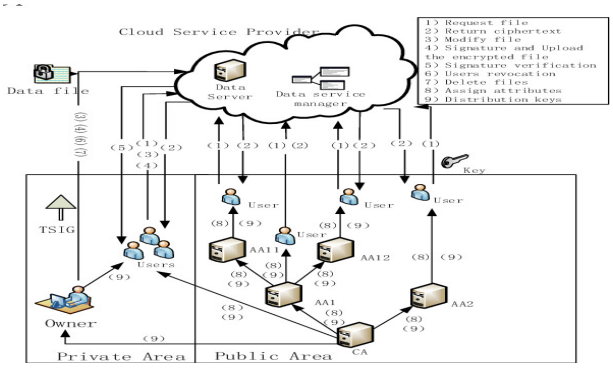


Fig 1. Example of Privacy Protection in Cloud Based Services

1. The data storage server and data service management are the two components of the cloud service provider. Data service administration is in responsibility of limiting external users' access to secret data and returning the associated ciphertext, while data storage servers are in charge of maintaining private data files.

2. In the real cloud environment, CA oversees several AA, and each AA oversees attributes in their respective fields.The traits that the user has come from various authorities.

3. The personal domain (PSD), which is accessible only to people with certain privileges such family, personal assistants, close friends, and partners. This domain is simple to maintain because it only includes a few users and a few small-scale attributes, and because the data owner is aware of each user's identity.

4. Public domain (PUD), which is home to a sizable number of users with ambiguous identities and a wealth of user-owned attributes.

5. Data Owner develops alternative access control strategies based on user characteristics in the public and private domains, encrypts submitted files using the appropriate encryption mechanism, and then sends the encrypted files to the cloud server.

IV. SYSTEM ARCHITECTURE DIAGRAM

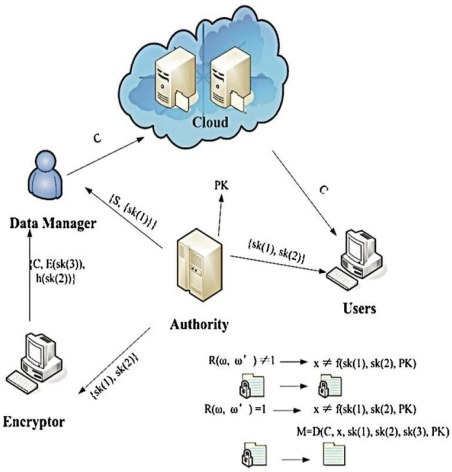


Fig.2. System Architecture

V.SYSTEM DESIGN

UML Diagram:

Unified Modelling Language is known as UML. A general-purpose modelling language with standards, UML is used in the field of object-oriented software engineering. The Object Management Group oversees and developed the standard. The objective is for UML to establish itself as a standard language for modelling object-oriented computer programmes. The Unified Modelling Language is a standard language for business modelling, non-software systems, and describing, visualising, building, and documenting the artefacts of software systems.

A.Class Diagram:

A class diagram in the Unified Modelling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among objects.

The class diagram is the main building block of object-oriented modeling. Class diagrams can also be used for data modeling. The classes in a class diagram represent both the main elements, interactions in the application, and the classes to be programmed.

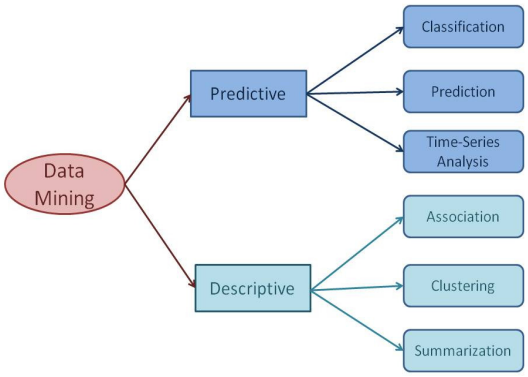


Fig.3 Class Diagram

B. Sequence Diagram:

A sequence diagram shows object interactions arranged in time sequence. It depicts the objects and classes involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario. Sequence diagrams are typically associated with use case realizations in the Logical View of the system under development. Sequence diagrams are sometimes called event diagrams or event scenarios.

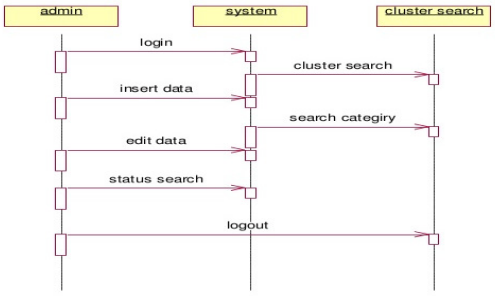


Fig.4 Sequence Diagram

C. Use Case Diagram:

A use case diagram at its simplest is a representation of a user's interaction with the system that shows the relationship between the user and the different use cases in which the user is involved. A use case diagram can identify the different types of users of a system and the different use cases and will often be accompanied by other types of diagrams as well.

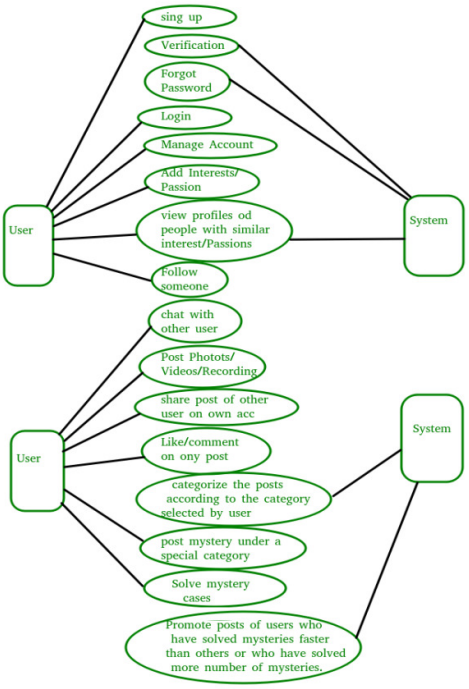
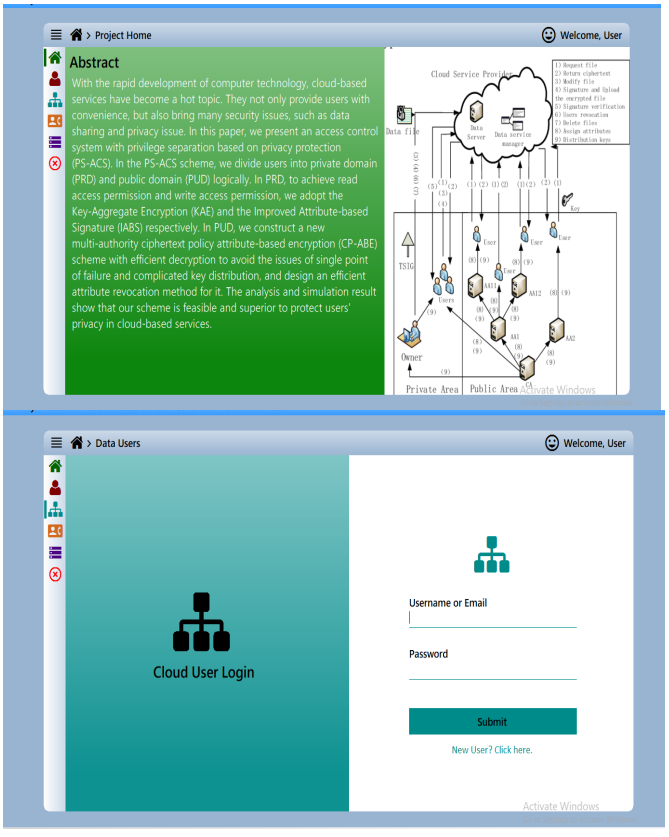
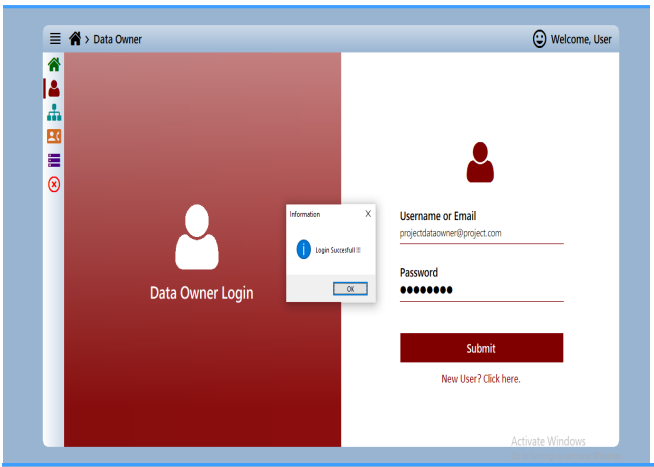
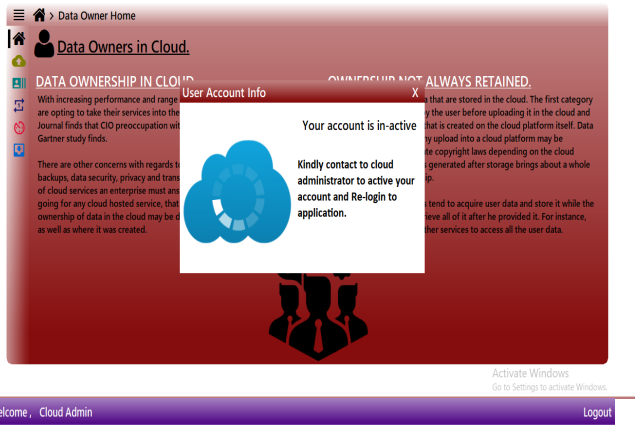


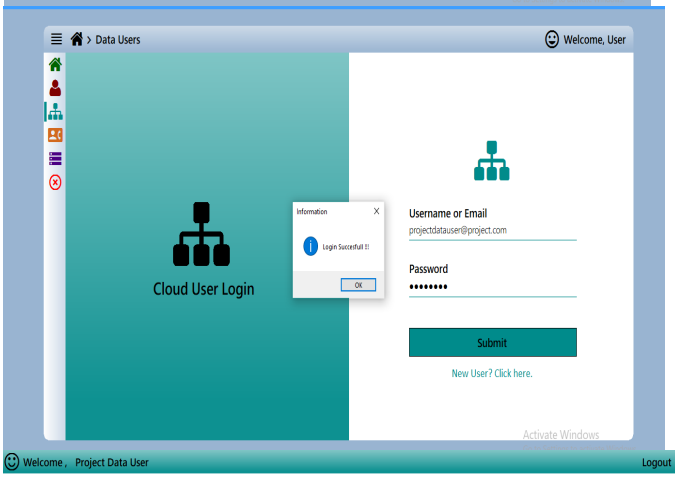
Fig.5 Use Case Diagram

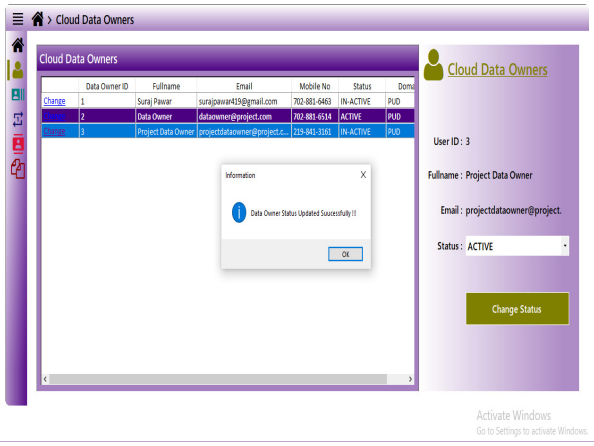
VI.RESULT

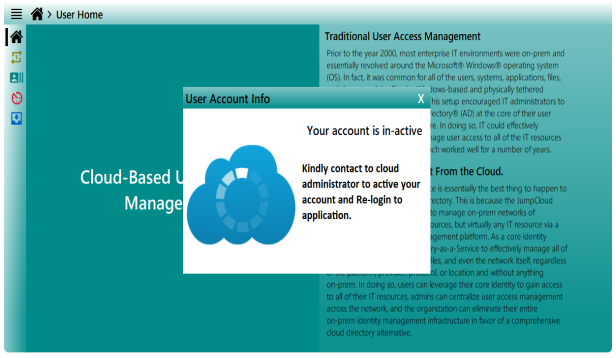


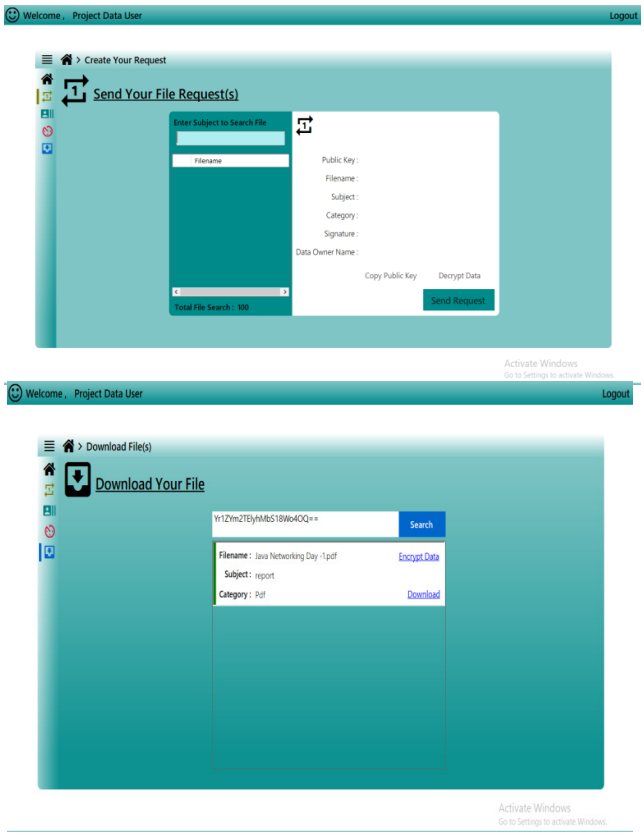












VII. CONCLUSION

In this research, we present the privilege separation based on privacy protection access control system (PS-ACS). We conceptually categorise users into personal domain (PSD) and public domain (PUD) by the examination of the cloud environment and user characteristics. The KAE algorithm is used in the PSD to implement read access permissions for users and significantly increased performance. The IABS technique is used to obtain write permissions and these encryptions of read and write permissions to safeguard user privacy. To prevent single points of failure and ensure data sharing in the PUD, we adopt the HABE scheme. The study also examines the scheme's effectiveness and security, and it provides simulation results. The suggested system demonstrates its excellence and viability in protecting the privacy of data in cloud-based services by comparison with the MAH-ABE scheme.

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] A. Lewko, B. Waters, "Decentralizing attribute-Based encryption," Proc. Advances in Cryptology-EUROCRYPT, 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. 131143, 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 - CT-RSA, pp. 376-392, 2011.

