Secure Data Group Sharing with Attribute and Time based Encrypted Data Access Over Cloud

[1]Dr B.GOPI, [2]D.NEELIMA, [3]M. PUSHPALATHA

[1]Associate Professor, Dept. of MCA, Krishna Chaitanya Institute of Science And Technology, Kakutur, Nellore, AP,India.

[2]PG Student, Dept. of MCA, Krishna Chaitanya Institute of Science And Technology, Kakutur, Nellore, AP,India.

[3]PG Student, Dept. of MCA, Krishna Chaitanya Institute of Science And Technology, Kakutur, Nellore, AP,India.

Abstract_ Cloud computing has become increasingly popular among users and organizations worldwide. Although cryptographic systems can provide data protection for users in the public cloud, some issues remain challenging, such as secure data group scattering and fine-grained access control of time-sensitive data. This paper proposes an identity-based data group sharing and dissemination scheme in the public cloud, where a data owner can broadcast encrypted data to a group of recipients by specifying their identities in a convenient and secure manner. To achieve secure and flexible data group dissemination, we adopt attribute-based and time-conditioned proxy re-encryption. This ensures that only data disseminators whose attributes satisfy the access policy of the encrypted data can spread it to other groups after the designated release time by assigning a re-encryption key to the cloud server. The re-encryption conditions are associated with attributes and release time, enabling the data owner to enforce fine-grained and scheduled release access control over the disseminated ciphertexts.

Index Terms—Attribute-based encryption, conditional proxy re-encryption, timed-release encryption, cloud computing

1.INTRODUCTION

Cloud computing is recognized as a computing paradigm where resources in the computing infrastructure are provided as services over the Internet. It benefits individual users and enterprises with convenient access, increased operational efficiencies, and rich storage resources by integrating a combination of existing and new techniques from research areas such as service-oriented architectures and virtualization. Despite the significant advantages offered by cloud computing, security concerns can impede its rapid development.

Increasingly, users are outsourcing their data to cloud service providers (CSPs) for sharing. However, CSPs, which deprive data owners of direct control over their data, are assumed to be honest-but-curious, raising security concerns.

These security issues in the public cloud necessitate effective measures to maintain data confidentiality. Various schemes utilizing cryptographic mechanisms have been proposed to address these security challenges. To ensure secure data group sharing, identity-based broadcast encryption (IBBE) is employed in the public cloud. Data owners can broadcast their encrypted data to a group of receivers simultaneously, using the public key, which can be an email, unique ID, or username. Thus, by leveraging an identity, data owners can securely and conveniently share data with other group users.

Attribute-based encryption (ABE) is a new cryptographic mechanism used in the cloud to achieve flexible and fine-grained secure data group sharing. Specifically, ciphertext-policy ABE (CP-ABE) allows data owners to encrypt data with an access policy, enabling only users whose attributes satisfy the policy to decrypt the data. Time-sensitive data, such as business plans and tenders, require time-based exposure. This means data owners may want different users to disseminate data at different times. For example, a data owner may share a sensitive business plan with directors and wish for these directors to disseminate the plan to managers at an early stage and to other employees at a later time..

2.LITERATURE SURVEY

1.TAFC: Time and Characteristic Variables Joined Admittance Control for Time-Touchy Information In broad daylight Cloud

assign expected clients and their important access honor delivering time focuses. It has been demonstrated that, in addition to realizing the function, owners, users, and the trusted CA bear only a negligible burden. It is introduced how to configuration access structure for any potential coordinated discharge access strategy, particularly implanting various delivering time focuses for various planned clients. Planned Delivery Encryption (TRE) turns into a promising crude, in which, a confided in time specialist, rather than information proprietors, consistently executes the timedrelease capability.

2. RAAC: Multiple Attribute

Authorities with Robust and Auditable Access Control for Public Cloud Storage Description: For public cloud storage, we propose a robust and effective heterogeneous framework with a single CA (Central Authority) and multiple AAs (Attribute Authorities) to address the single-point performance bottleneck of key distribution in the existing schemes. The weighty heap of client authenticity check is shared by numerous AAs, every one of what man-ages the all inclusive trait set and can autonomously complete the client authenticity confirmation, while CA is just liable for computational undertakings. For the first time, a heterogeneous access control framework has been proposed as a solution to the single-point performance bottleneck and low efficiency of cloud storage. It is reproduced the CP-ABE plan to accommodate our proposed structure and propose a hearty and high-proficient access control plot, in the mean time the plan actually protects the fine granularity,

adaptability and security highlights of CP-ABE.

3.PROPOSED WORK

The essential objective of our plan is to accomplish fine-grained and coordinated discharge information bunch dispersal. Fig. 1 shows the framework model of our plan, which comprises of the accompanying framework elements.

□ The focal power (CA) is a completely confided in au-thority running on confided in cloud stage with adaptability and versatility that oversees and dis-tributes open/mystery enters in the framework, including creates framework parameters to instate sys-tem and produces private keys and quality keys with clients' character and characteristics. Likewise, it goes about as a confided in time specialist to distribute time token at each pre-characterized time.

□ The CSP is a semi-confided in substance that has rich stockpiling limit and calculation influence to master vide information sharing administrations in broad daylight cloud. It is accountable for controlling the gets to from outside us-ers to the put away information and giving compare ing administrations. At the point when it gets the solicitation of information re-encryption, it is answerable for creating a re-scrambled ciphertext with re-encryption key from information disseminator. Consequently, CSP stores initial ciphertexts, yet in addition re-scrambled ciphertexts.

 The information proprietor wishes to redistribute the information into cloud for comfort of gathering sharing and dissemination. The information proprietor is accountable for encrypting information for a lot of collectors. On the off chance that the information proprietor has the prerequisite to confine his information to be dispersed by some particular individuals after some particular time, the information proprietor can characterize at-tribute-based and planned discharge get to approach, and uphold it all alone information by scrambling the information under the arrangement before re-appropriating it.

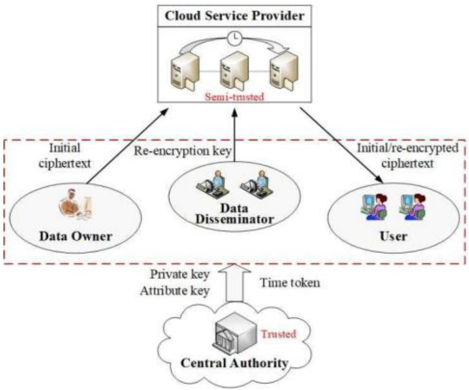
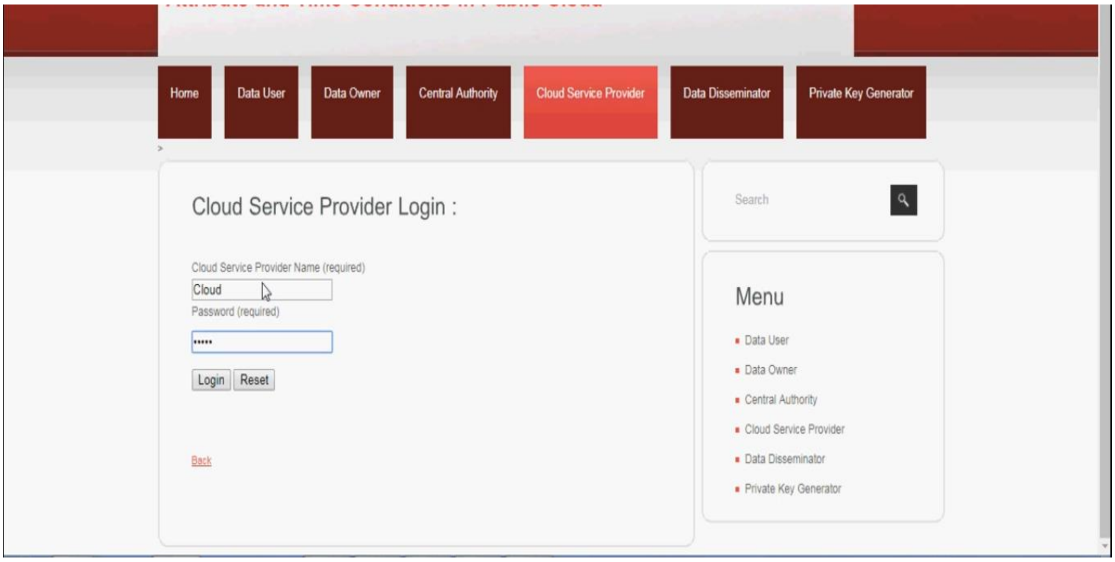


Fig 1: Proposed Model

The information disseminator is the individual who wishes to share information proprietor's information with others (for example his companions, relatives, partners). Data disseminator must be one of the owner's designated intended receivers for security and access control purposes, and they must be able to decrypt the initial ciphertexts. In order to distribute the owner's data to other parties, the data disseminator can generate re-encryption keys and send data re-encryption requests to the CSP with these keys. Just the qualities of information disseminator fulfill access strategy and the pre-decided time shows up, information re-encryption solicitation can be effectively executed by CSP. The outsourced data can be accessed by the user, who is the ciphertexts receiver. The client can decode the underlying and yet again encoded ciphertexts assuming he is the in-tended beneficiary characterized by the information proprietors or information disseminators.

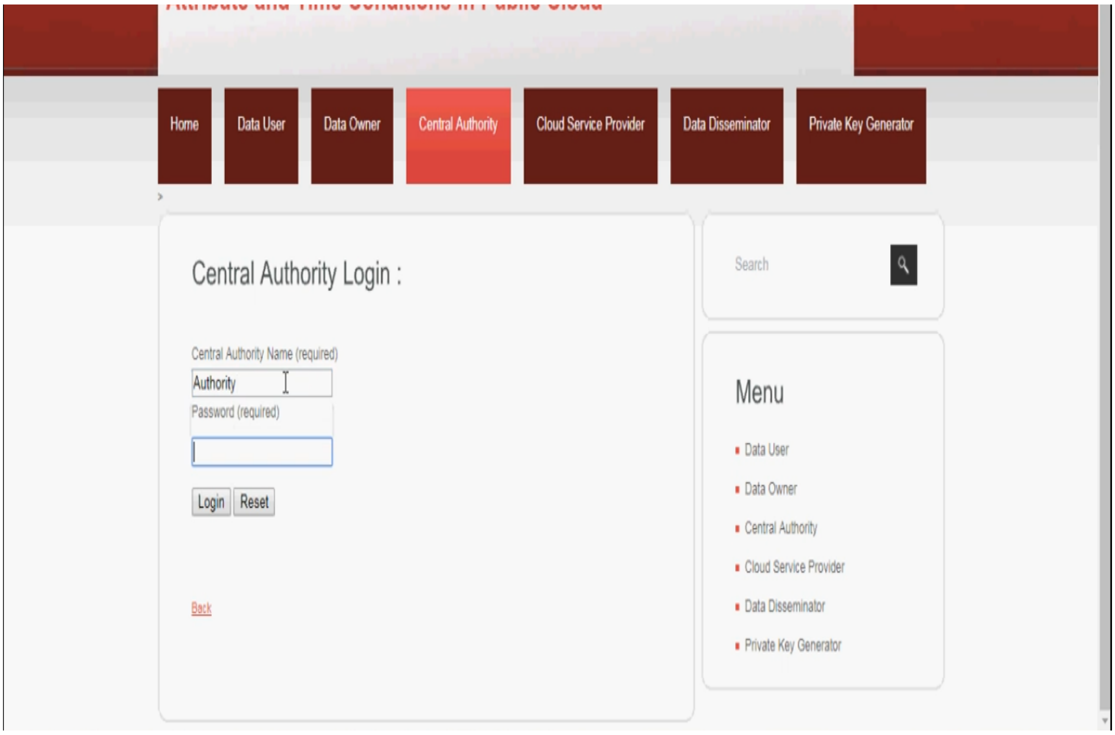
4.RESULTS AND DISCUSIONS



Cloud Service Provider Login :

Cloud Service Provider Name (required)
Cloud
Password (required)
•••••

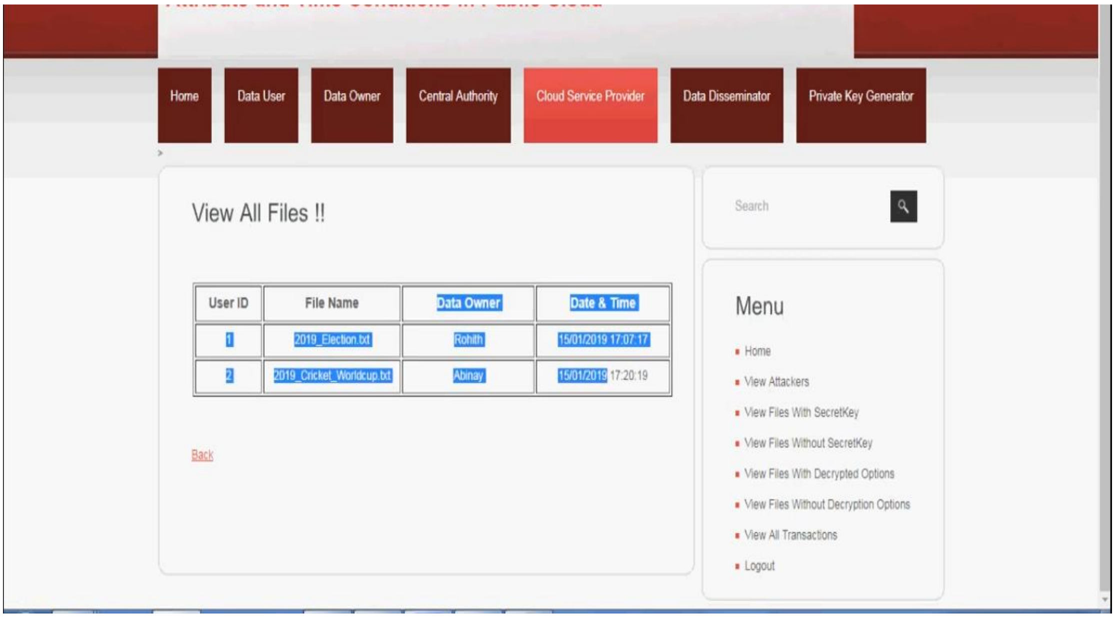
Fig 1: Cloud Server Provide Login Page



Central Authority Login :

Central Authority Name (required)
Authority
Password (required)

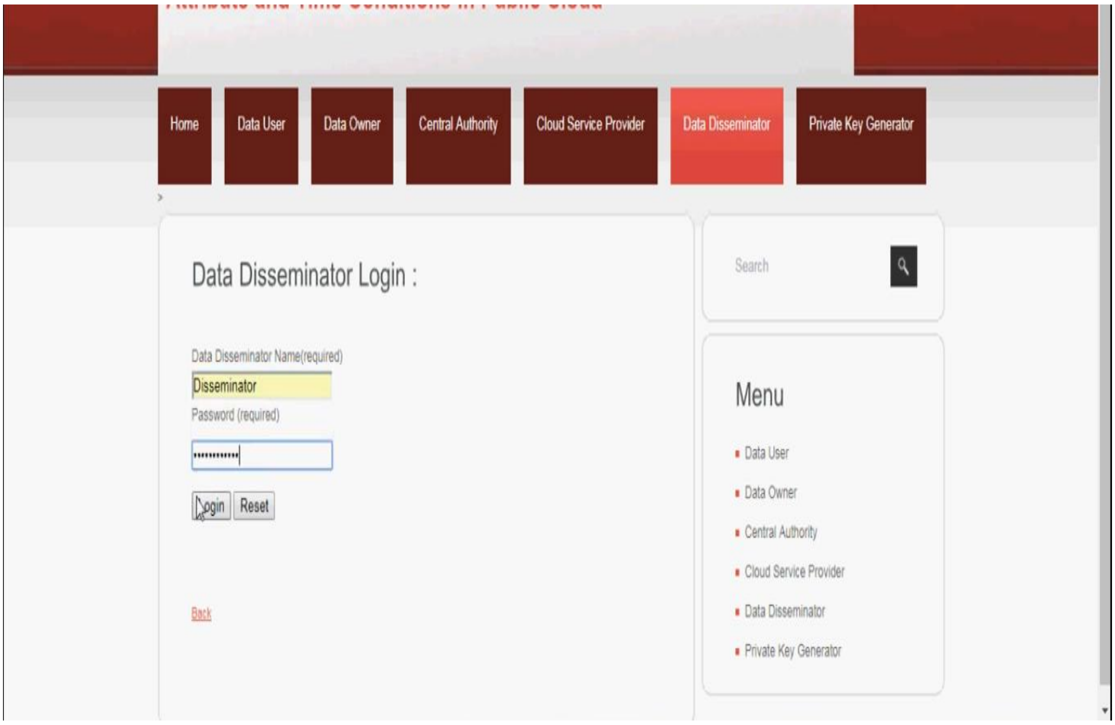
Fig 2: central authority page



View All Files !!

User ID	File Name	Data Owner	Date & Time
1	2019_Election.txt	Rohith	15/01/2019 17:07:17
2	2019_Cricket_Worldcup.txt	Abinay	15/01/2019 17:20:19

Fig 3: view all files



Data Disseminator Login :

Data Disseminator Name(required)
Disseminator
Password (required)
•••••••••••

Fig 4: data disseminator page

5.CONCLUSION

In this paper, propose a secure information bunch sharing and scattering plan out in the open cloud dependent on at-tribute-based and planned discharge restrictive personality based communicate PRE. Our plan enables clients to impart information to a gathering of beneficiaries by utilizing character, for example, email and username at once, which would ensure information sharing security and accommodation out in the open cloud. In addition, with the use of fine-grained and planned discharge CPRE, our plan enables information proprietors to custom access arrangements and time trapdoors in the ciphertext which could restrain the dispersal conditions while re-appropriating their information. The CSP will re-encode the figure message effectively just when the qualities of information disseminator related with the re-encryption key fulfill get to strategy in the underlying ciphertext and the time trapdoors in the underlying figure content are uncovered. We lead our tests with matching based cryptography library. The hypothetical analaysis and trial results have demonstrated the security and effectiveness of our plan

REFERENCES

[1] K. Ren, C. Wang, and Q. Wang, ―Security Challenges for the Public Cloud,‖ *IEEE Internet Computing*, vol. 16, no. 1, pp. 69-73, 2012.

[2] C. Delerablée, ―Identity-based Broadcast Encryption with Constant Size Ciphertexts and Private Keys,‖ *Proc. the 13th International Confer- ence on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2007)*, pp. 200-215, 2007.

[3] F. Beato, S. Meul, and B. Preneel, ―Practical Identity-based Private Sharing for Online Social Networks,‖ *Computer Communications*, vol. 73, pp. 243-250, 2016.

[4] J. Bethencourt, A. Sahai, and B. Waters, ―Ciphertext-policy Attribute-based Encryption,‖ *Proc. the 28th IEEE Symposium on Security and Pri- vacy (S&P 2007)*, pp. 321-334, 2007.

[5] Z. Wan, J. Liu, and R. Deng, ―HASBE: A Hierarchical Attribute-based Solution for Flexible and Scalable Access Control in Cloud Compu- ting,‖ *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 743-754, 2012.

[6] H. Hu, G. Ahn, and J. Jorgensen, ―Multiparty Access Control for

Online Social Networks: Model and Mechanisms,‖ *IEEE Transactions on Knowledge and Data Engineering*, vol. 25, no. 7, pp. 1614-1627, 2013.

[7] M. Blaze, G. Bleumer, and M. Strauss, ―Divertible Protocols and Atomic Proxy Cryptography,‖ *Proc. Advances in Cryptology-EUROCRYPT 1998 (EUROCRYPT '98)*, pp.127-144, 1998.

[8] D. Tran, H. Nguyen, W. Zha, and W. Ng, ―Towards Security in Sharing Data on Cloud-based Social Networks,‖ *Proc. the 8th International Conference on Information, Communications and Signal Processing (ICICS2011)*, pp. 1-5, 2011.

[9] J. Weng, R. Deng, X. Ding, C. Chu, and J. Lai, ―Conditional Proxy Re- Encryption Secure Against Chosen-ciphertext Attack,‖ *Proc. the 4th International Symposium on ACM Symposium on Information, Computer and Communications Security (CCS 2009)*, pp. 322-332, 2009.

[10] P. Xu, T. Jiao, Q. Wu, W. Wang, and H. Jin, ―Conditional Identity-based Broadcast Proxy Re-encryption and its Application to Cloud Email,‖ *IEEE Transactions on Computers*, vol. 65, no. 1, pp. 66-79, 2016.