Hybrid Approach for Public Cloud Stored Data

[1]Mr. Swapnil Wani [2]Miss.Sayali Gholap, [3]Mr.Yash Andhalkar, [4]Mr.Akhil Singh
[1]Asst.Professor,[2,3,4]UG Student,[1,2,3,4]Computer Engg. Dept. Shivajirao S. Jondhle
College of Engineering & Technology, Asangaon, Maharshatra, India. [1]*swapnilwani27@hotmail.com*
,[2]*gholaps143@gmail.com*,[3]*yashandhalkar@gmail.com*, [4]*singhakhilmi@gmail.com*

Abstract- The new paradigm of outsourcing data to the cloud is a double-edged sword. On the one hand, it frees data owners from the technical management, and is easier for data owners to share their data with intended users. On the other hand, it poses new challenges to privacy and security protection. To protect data confidentiality against the honest-but-curious cloud service provider, numerous works have been proposed to support fine-grained data access control. However, till now, no schemes can support both fine-grained access control and time-sensitive data publishing. In this, by embedding timed-release encryption into CP-ABE (Ciphertext-Policy Attribute-based Encryption), a new time and attribute factors combined access control on time-sensitive data for public cloud storage (named TAFC). Based on the proposed scheme, propose an efficient approach to design access policies faced with diverse access requirements for time-sensitive data. Extensive security and performance analysis that proposed scheme is highly efficient and satisfies the security requirements for time-sensitive data storage in public cloud.

Keywords: Cloud Storage, Data security, Fine-grained Access control, Timed-release encryption, CP-CBE (Ciphertext Policy Attribute Based Encryption).

I. INTRODUCTION

Computer security (Also referred to as cyber security or IT Security) is data security as applied to computers and networks. the sphere covers all the processes and mechanisms by that computer-based instrumentation, data and services are protected against uncaused or unauthorized access, amendment or destruction. pc security conjointly includes protection from unplanned events and natural disasters. Otherwise, within the industry, the term security or the phrase pc security refers to techniques for making certain that information keep in an exceedingly pc can't be scan or compromised by any people while not authorization. Most pc security measures involve encoding and passwords. encoding is that the translation of knowledge into a type that's unintelligible while not a deciphering mechanism. A parole could be a secret word or phrase that provides a user to a selected program or system. Cloud storage service has important blessings on each convenient information sharing and price reduction. However, this new paradigm storage brings concerning new challenges concerning data confidentiality protection. In reality, the time issue sometimes plays a very important role in managing time sensitive information.

II. AIM AND OBJECTIVE

a) Aim

Malicious user is to win over the cloud server that he's a legitimate information owner.to style a dynamic collaboration surroundings utilizing the advantages of cloud storage whereas making certain sturdy information security and fine-grained information access.to enhance our skills and data with regards to coming up with systems that leverage them edges of the cloud, improve our ability to analysis a scientific subject from totally different views, and to contribute to the scientific community

b) Objective

Access control Improving data confidentiality in cloud storage environments while enhancing dynamic sharing between users. Indeed, the proposed security mechanisms should ensure both robustness and efficiency, namely the support of flexible, efficient user revocation and performances.

III. LITERATURE SURVEY

Paper 1:- "survey of proxy encryption for secure data sharing in cloud computing".

Never before have data sharing been more convenient with the rapid development and wide adoption of cloud computing. However, how to ensure the cloud user's data security is becoming the main obstacles that hinder cloud computing from extensive adoption. Proxy re-encryption serves as a promising solution to secure the data sharing in the cloud computing. It enables a data owner to encrypt shared data in cloud public key, which is further transformed by a semi trusted cloud server into an encryption intended for the legitimate recipient for access

 DOI : 10.35291/2454-9150.2020.0231

control. A parole could be a secret word or phrase that provides a user to a selected program or system.

paper 2:- "transparent data deduplication in the cloud."

Cloud storage providers such as Drop box and Google drive heavily rely on data DE duplication to save storage costs by only storing one copy of each uploaded file. Although recent studies report that whole file DE duplication can achieve up to 50% storage reduction, users do not directly benefit from these savings-as there is no transparent relation between effective storage costs and the prices offered to the users.

Paper 3:- cloud authorization: exploring techniques and approach towards effective access framework control.

present how to design access structure for any potential timed-release access policy, especially embedding multiple releasing time points for different intended users.

IV. EXISTING SYSTEM

The new worldview of outsourcing information to the cloud is a twofold edged sword. From one viewpoint, it liberates information proprietors from the specialized administration and is less demanding for information proprietors to impart their information to proposed clients. On the other hand, it postures new difficulties on security and security assurance. In a TRE-based system, a trust time agent, rather than data owner, can uniformly release the access privilege at a specific time. It has been proposed to integrate TRE into remote data access control. It made a preliminary attempt to integrate time with attributes, but it only addresses the issue that the attributes' life period of each user is limited by time.

V. COMPARTIVE STUDY

SR NO.	PAPER TITLE	AUTHOR NAME	TECHNOLOGY	ADVANTAGE	DISADVANTAGE
1	Survey of proxy encryption for secure data sharing in cloud computing	Z. Qin, H. Xiong, S. Wu, and J. Baramulla IEEE, 2013.	CPABE (Cipher text- Policy Attribute based Encryption)	By integrating TRE and CPABE in public cloud storage, propose an efficient scheme to realize secure fine-grained access control for time sensitive data.	CP-ABE determines users' access privilege based only on their inherent attributes without any other critical factors
2	Transparent data deduplication in the cloud	F.Armknecht, J.-M. Bohli, G. O. Karame, and F. Youssef. IEEE, 2014	TRE algorithm	In the proposed scheme, the data owner can autonomously designate intended users and their relevant access privilege releasing time points.	These schemes cannot support gradual access privilege releasing
3	cloud authorization: exploring techniques and approach towards effective access control framework	R. Masood, M. A. Shibli, Y. Ghazi, A. Kanwal, and A. Ali. IEEE, 2015.	Time release encryption	present how to design access structure for any potential timed-release access policy	These schemes either lack fine-grained access control or leave an unbearable burden.
4	Hybrid Approach for Public Cloud Stored Data	F. Armknecht, J.-M. Bohli, G. O. Karame, and F. Youssef	Time release encryption	Access structure for any potential regular discharged access policy, especially.	These schemes cannot support gradual access privilege releasing

VI. PROBLEM STATEMENT

That problem is explained from Cloud Service Provider perspective, because the problems to the virtual machines raises at Cloud service providers site and it may affect both cloud service providers as well as cloud service users. When the virtual resources are formed out of available actual physical resources, those virtual resources may face the problems from intruders, malwares or sometimes the virtual machines themselves corrupted and in turn they trouble the other virtual machines, and also make those virtual machines to consume more resources like processing power, memory and bandwidth etc.

VII. PROPOSED SYSTEM

This system proposed an efficient time and attribute factors combined access control scheme, named Hybrid Approach for Public Cloud Stored Data, for time-sensitive data in public cloud. This possesses two important capabilities: 1. It inherits the property of fine granularity from CP-ABE 2. By introducing the trapdoor mechanism, it further retains the feature of time release from TRE. classifier and neural network are used in proposed system.

VIII. ALGORITHM

1) Setup: Here is the depth of key structure. Take as input a parameter. It output a public key PK and master secret key MK.

Input: P ε G1 and Q ε G2 a set of attribute H Output: Public Key PK(G1,G2,P,Q,P δ, γ) , { H1……HN} , Master private Key MK(Pα).

1: Choose at random : α and δ ε Z
2: Pδ ← [δ]P
3: Pα ← [α]P
4: γ ← (Q,P) α
5: for i ← 1 to # H do

 DOI : 10.35291/2454-9150.2020.0231

6: Generate a point Hi ε G1
7: end for
8: PK ← (G1,G2,P,Q,P δ, γ) , {H1……HN}
9: MK ← (Pα)
10: return PK,MK

IX. MATHEMATICAL MODEL

Setup: CA generates I =[p, G1, G2, g, e, H1, H2, FT] where e : G1 ×G1 → G2 is a bilinear map, G1 and G2 are cyclic multiplicative.

Groups of a prime order p, g is a generator of G1, H1 : {0,1}∗ → G∗ 1, H2 : G∗ 2 → Z∗ p.

FT is the time format.

CA randomly chooses α, β, γ ∈ Z∗ p. The public parameter is published as: and the master key MK is (β,γ,gα), which implicitly exists in the system, and doesn't need to be obtained by any other entity.

(Note that f and γ are used for timed-release function.)

X. SYSTEM ARCHITECTURE

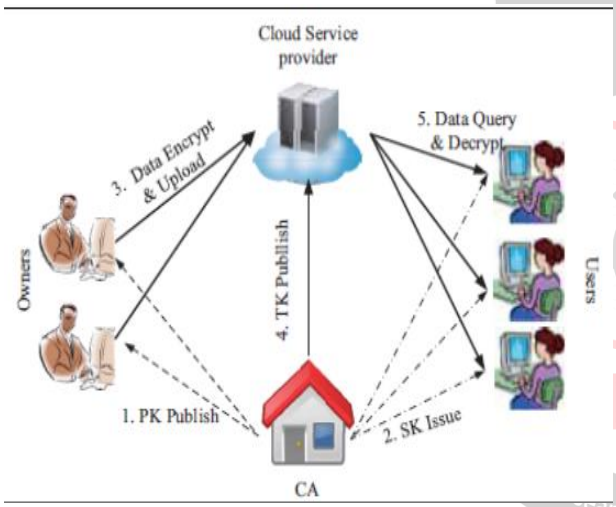

Fig.1: System Architecture

XI. ADVANTAGES

By integrating TRE and CP-ABE in public cloud storage, propose an efficient to realize secure fine-grained access control for time-sensitive data.

• In the system, the data owner can autonomously designate intended users and their relevant access privilege releasing time points. Besides realizing the function, it is proved that the negligible burden is upon owners, users and the trusted CA.

• Access structure for any potential timed released access policy, especially embedding multiple releasing time points for different intended users.

• Furthermore, a rigorous security proof is given to validate that the proposed system is secure and effective.

proved that the negligible burden is upon owners, users and the trusted CA.

• Access structure for any potential timed released access policy, especially.

XII. DESIGN DETAILS

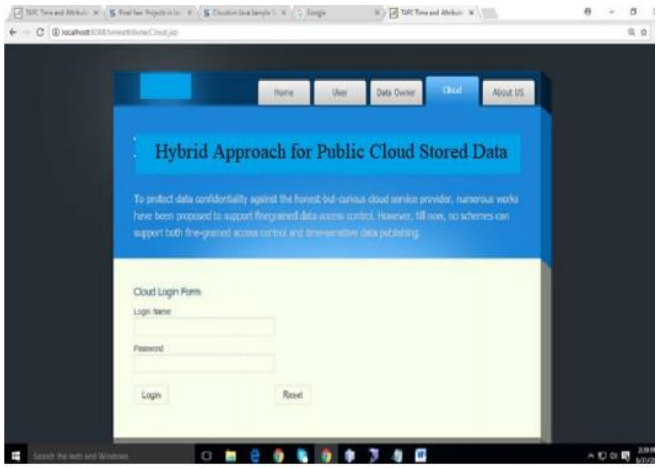

Fig 2: Cloud Home Page for Hybrid Approach for Public Cloud Stored Data.

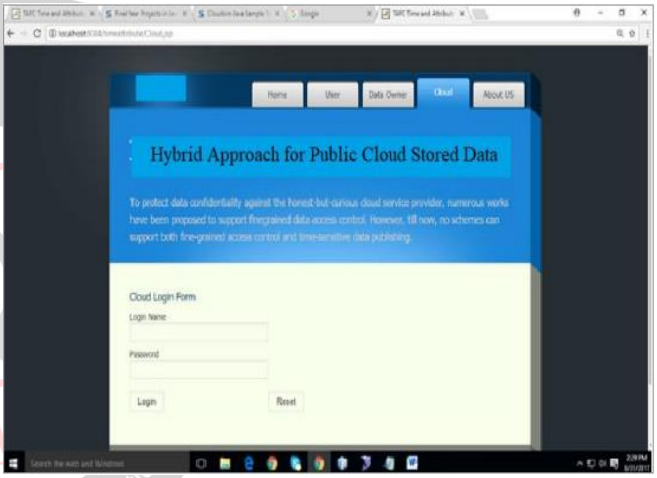

Fig: 3: Data owner Login Page for Hybrid Approach for Public Cloud Stored Data

XIII. CONCLUSION

Thus, we have tried to implement the paper "Jianan Hong, Kaiping Xue TAFC: Time and Attribute Factors Combined Access Control for Time-Sensitive Data in Public Cloud "IEEE (2017). and according to implementation the conclusion of Hybrid Approach for Public Cloud Stored Data are as follows. It aims at fine-grained access control for time sensitive data in cloud storage. One challenge is to simultaneously achieve flexible timed release and fine granularity with lightweight overhead, which is not provided in related work time. The analysis shows that it can protect the confidentiality of time-sensitive data, with a lightweight overhead on both CA and data owners, thus well suits the practical large-scale access control system for cloud storage the practical large-scale access control system.

 DOI : 10.35291/2454-9150.2020.0231

REFERENCE

[1] Z. Qin, H. Xiong, S. Wu, and J. Batamuliza, "A survey of proxy re-encryption for secure data sharing in cloud computing," IEEE Transactions on Services Computing, Avaliable online, 2016.

[2] F. Armknecht, J.-M. Bohli, G. O. Karame, and F. Youssef, "Transparent data deduplication in the cloud," in Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pp. 886–900, ACM, 2015.

[3] R. Masood, M. A. Shibli, Y. Ghazi, A. Kanwal, and A. Ali, "Cloud authorization: exploring techniques and approach towards effective access control framework," Frontiers of Computer Science, vol. 9, no. 2, pp. 297– 321, 2015.

[4] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.

[5] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertextpolicy attribute-based encryption," in Proceedings of the 28th IEEE Symposium on Security and Privacy (S&P '07), pp. 321–334, IEEE, 2007.

[6] Z. Wan, J. Liu, and R. H. Deng, "HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 743–754, 2012.

 DOI : 10.35291/2454-9150.2020.0231