IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 44-48

Efficient & Secure Cloud Computing With Time and Attribute Factor Combined Access Control

Paurnima Prakash Kawale[1], Prof. Roshani Talmale[2]
1M.Tech Scholar, Department of Computer Science and Engineering Tulsiramji Gaikwad-Patil College of Engineering and Technology Nagpur, Maharashtra, India
2 Dept. of Computer Science and Engineering Tulsiramji Gaikwad-Patil College of Engineering and Technology Nagpur, Maharashtra, India

Abstract: *When it comes to storing data, cloud storage is rapidly turning into the procedure for choice. Cloud storage isquickly becoming the strategy for decision. Putting away files remotely instead of by locally boasts an array of preferencesfor both home and professional clients. Cloud storage means "the storage of data online in the cloud", However, the cloudstorage is not completely trusted. Whether the data put away on cloud are in place or not turns into a significant concernof the clients also access control becomes a difficult job, particularly when we share data on cloud servers. To tacklethis issue Time and Attribute Factors Combined Access Control for Time-Sensitive Data in Public Cloud scheme is introduced. we further propose an efficient approach to design access policies faced with diverse access requirements for time-sensitive data. In this system, each ciphertext is labeled with a time interval. If the attributes associated with theciphertext satisfy the key's access structure and both the time instant is in the allowed time interval, then the ciphertextis decrypted. After a user-specified end time the data at cloud server will not be available. Extensive security and performance analysis shows that our proposed scheme ishighly efficient and satisfies the security requirements for time sensitive data storage in public cloud.*

Index Terms: *Attribute Based Encryption, Cloud computing, Time and Attribute Factors Combined Access Control*

I. Introduction

Cloud computing alludes to the usage of computing resources, those being programmingor equipment that reside on a remote machine and are conveyed to the end client as an service over a system, with the most common example being the web. Cloud storage is gaining popularity and importance very rapidly. To share data securely the attribute based encryption technique or use of combination of attribute is used. The attribute-based encryption (ABE) is a significant primitive of Attribute-based cryptography. As such it is a kind of public-key encryption in which the public key of a user is several unique information about the attribute (e.g. a company name). This means that a sender who hasaccess to the public parameters of the system can encrypt a message using e.g. the text value of the receiver's email address as a key.

In Attribute Based Encryption each user is identified by a set of attributes. Every cipher text in ABE is associated with particular set of attributes and it can be only decrypted by user who has access to corresponding secret key. The master secret key holder can extract a secret key and securely shares with user who satisfies the access control policies defined by data owner basedon attributes of users.

Cloud storage is becoming very emerging now a days. Online data almost always available in shared environments so that, ensuring privacy is a very vital task. Nowadays, many online services are available that are using personal data. Any user can easily apply for free accounts for email, photos, files etc. with specified storage space. Also with the help of wireless technology users are accessing their files, emails by their mobiles from anywhere. Traditionally, data privacy was provided by depending on server ensuring access control mechanism and authentication but, in this any unexpected privilege escalation will expose all data. Solution for this is to encrypt data before uploading to cloud storage.

Relying on numerous techniques such as cryptographic primitives, there have been lots of research on data sharing in cloud storage securely. Some techniques, focused at protecting the integrity of the shared data and some on protecting the confidentiality and access control of the data. In data access control, ABE is used as a basic cryptographic method. These ABE-based access control schemes, in general, can be categorized into key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). The next one is more relevant for achieving flexible and fine-grained access control for the public cloud, in which each file is labelled with an access structure, and each user have a security key embedded with a set of attributes.

Also to improve the cloud storage space a secure data self-destructing system in cloud computing is proposed. In this system, while private key is connected with a time instant each ciphertext is labeled with a time interval. If both the time instant is in the allowed time interval and the identities associated with the

ciphertext satisfy the key's access structure then the ciphertext can be decrypted. In general, the owner has the right to specify that certain sensitive information is only valid for a limited period of time i.e. self-destructed after completion of time interval set by the owner, or should not be unconfined before an exacting time.

In order to build a scalable and fine-grained access control system for deployed time-sensitive data, CP-ABE and TRE cryptographic techniques are added together. First is used to give an expressive access control primitive with fixed attribute sets; and the next one is to realize timed-release function apart from attributes and logic gates defined in previous CP-ABE, the access structure of proposed scheme consist more than one timetrapdoors (*TS*), each of which indicate a time point. The trapdoor is developed for the timed release function in CP-ABE algorithm,it can be deployed on any node in the structure, arbitrarily stating access privilege releasing time for numerous users. The accessing time with user's attribute set estimates whether the user satisfies the policy. For each shared file, the data owner estimates the access policy (AP) to encrypt the file. Especially, the time trapdoors in the policy are created based on a time point.

The section I explains the Introduction of Time and Attribute Factors Combined Access Control. Section II presents the literature review of existing systems and Section III present proposed system Section IV presents experimental analysis of proposed system. Section V concludes our proposed system. While at the end list of references paper are presented.

II. Literature Review

A. Boldyrevaet al. [3] proposed the Identity-based encryption, as IBE eliminates the need for a Public Key Infrastructure (PKI), it is an exciting alternative to public-key encryption. Any setting, PKI- or identity-based, must give a means to revoke users from the system. Proficient revocation is a well-studied difficulty in the traditional PKI setting. However in the setting of IBE, there has been little work on studying the revocation mechanisms. When encrypting, the most practical solution need the senders to also use time periods and by contacting the trusted authority all the receivers to update their private keys regularly. But this solution does not scale well the work on key updates becomes a bottleneck, as the number of user's increases. We propose an IBE scheme that appreciably progresses key-update effectiveness on the side of the trusted party, while staying proficient for the users. Our system constructs on the ideas of the Fuzzy IBE primitive and binary tree data structure, and is provably secure.

D. Boneh and M. Franklin[4] suggests a fully functional identity based encryption scheme (IBE). Assuming a variant of the computationalDiffie Hellman problem the system has selectedciphertext security in the random oracle model. The system is based on bilinear maps between groups. The Weil pairing on elliptic curves is an example of such a map.

A. Sahaiet al. [5] studied that the kind of IBE plan that call as Fuzzy Personality Based Encryption. In Fuzzy IBE a way of life as set of illustrative qualities are used. A Fluffy IBE plan takes into account a private key for a personality, !, to unscramble a cipher text scrambled with a personality, !0, if and just if the characters ! What's more, 0 are near one another as measured by the "set cover" separation metric. A Fuzzy IBE plan can be connected to empower encryption utilizing biometric inputs as personalities; the blunder resistance property of a Fuzzy IBE plan is correctly what takes into accountthe utilization of biometric personalities, which inalienably will have some commotion every time they are inspected. Moreover, we demonstrate that Fuzzy-IBE can be utilized for a sort of application that we term "quality based encryption".Fuzzy IBE allows to one single compressed secret key to decrypt cipher texts those are encrypted under many identities which are near about close in specific manner. Fuzzy IBE allows private key as identity and to decrypt cipher text encrypted with identity only if those identities are close to each other. Fuzzy IBE can also shows encryption using biometric inputs as identities

J. Liet al. [6] addresses the problemsof utilizing untrusted cryptographic partners. A formal security definition to safely outsourcing calculations from a computationally constrained gadget to an untrusted partner is proposed. In this model, the will disposed environment composes the product for the partner, however then does not have direct correspondence with it once the gadget begins depending on it. Not with standing security, it likewise gives a structure to measuring the effectiveness also; check ability of an outsourcing usage. It also introduce two pragmatic outsource secure plans. In particular, it demonstrate to safely outsource measured exponentiation, which presents the computational bottleneck in most open key cryptography on computationally restricted gadgets. Without outsourcing, a gadget would require O(n) particular augmentations to complete particular exponentiation forn-bit types. The heap lessens to O (log2 n) for any exponentiation based plan where the genuine gadget may utilize two untrusted exponentiation programs; they highlight the Cramer-Shoup cryptosystem and Schnormarks as samples. With a casual thought of security, we accomplish the same burden diminishment for another CCA2-secure encryption plan utilizing stand out untrusted Cramer Shoup encryption program.

B. Zhang[7] demonstrated that the ABE is a promising cryptographic apparatus for engrained access control. Be that as it may, the computational taken at online encryption ordinarily develops with them any-sided

quality of access arrangement in existing ABE plans, which turns into a bottleneck constraining its application. In this paper, a novel worldview of outsourcing encryption of ABE to cloudadministration supplier to calm neighborhood calculation trouble is proposed. It utilizes an enhanced development with MapReduce cloud which is secure under the suspicion that the expert hub and in addition at minimum one of the slave hubs is straightforward. In the wake of outsourcing, the computational taken a toll at client side amid encryption is decreased to inexact four exponentiations, which is steady. Another point of preference of the proposed development is that the client can assign encryption for any arrangement.

J. Li et al. [8] proposed ABE scheme, ABEis a promising cryptographic primitive, which has been widely applied to design fine-grained access control system recently. Though, ABE is being criticized for its high scheme overhead as the computational cost grows with the complexity of the access formula. Because they have constrained computing resources this disadvantage becomes more serious for mobile devices. Aiming at attempting the above confront, it presents a general and proficient solution to apply attribute-based access control system by establishes secure outsourcing methods into ABE. More exactly, two cloud service providers (CSPs), namely key generation-cloud service provider (KG-CSP) and decryption-cloud service provider (D-CSP) are establish to perform the outsourced key-issuing and decryption on behalf of attribute authority and users respectively.

R. Canetti[9] proposed the prototype of forward security for Cryptographic computations was introduced. Secret keys are updated at usual periods of time; contact of the secret key matching to a given time period does not allow an challenger to "break" the scheme for any previous time period in a forwardsecure scheme. A number of constructions of forward-secure digital signature schemes, key-exchange protocols, and symmetric-key schemes are known. The main building attains security beside chosen-plaintext attacks under the decisional bilinear Diffie-Hellman supposition in the standard model. This system is practical, and with the total number of time periods all parameters grow at most logarithmically

Most efficient techniques for access control of online data is utilization of pre-defined hierarchy of secret keys [10] i.e. in the form of tree structure. In tree structure key assigned to a particular node is used to derive the keys of its descendent nodes i.e. granting the access to key corresponding to any node implicitly gives access to all keys to its descendent nodes. This technique decreasing the expense in storing and managing secret keys.

Sandhu et al. [11] proposed a method to generate a tree hierarchy to define access control using symmetric keys. With this scheme information is classified into classes and these classes are managed as a rooted tree i.e. hierarchy. In this tree most privileged security class is at the root. User stores a single key of fixed size associated to its security class and keys for the security classes in the subtree are created from this key by using one-way functions.

This encryption scheme [13] is invented for sharing number of keys at a time in broadcast scenario. Data Encryptor that is Owner needs to get the respective secret key for encryption of data trough secure channel. This key sharing via secure channel is costly and not always suitable for many applications on cloud.

III. System Architecture

A. System Architecture

Here Fig.1 shows the proposed architecture which depict the ciphertexts are transmitted from data owners to the cloud, and users can query any data. *CA* controls the system with the operations: 1) It assign security keys to each user, according to user's attribute set; 2) At each time point, it publishes a time token (*TK*), which is utilized to grant access privilege to users for accessing the data.

Fig 1. System Architecture

B. Proposed System

System architecture consists of the following entities: a central authority (*CA*), several data owners (Owner), many data consumers (User), and a cloud service provider (Cloud).We design Attribute-Based

Encryption scheme based on Public Key Encryption which is efficient and flexible in the sense that any subset of cipher texts is decryptable by decryption key of constant size which also called as attribute key. CA manages the security protection of the complete system. It assigns system parameters and gives security keys to each user. It alsowork as a time agent to manage the timed-releasing function.Ownerdecides the access policy (AP) depends on a specific attribute set and one or more releasing time intervals for each file, and then encrypts the file based policy before uploading it.CA assign a security key to user. User can query any data or file stored on cloud, but is able to decrypt it only if his attribute set similar the AP and the current access time is later than the specific releasing time.Cloud provides services to user based on CA control.

Data owner encrypts all files with the public key and also with the attribute for that cipher text. Data owner also contains master secret key from which different secret keys for cipher text classes can be extracted. With this solution, data owner encrypts all files under the attribute for the cipher text. Receiver then downloads the specific files from cloud storage and uses key assigned by CA to decrypt these files. Also the file has time limit to access hence specific time to access the file is granted to user. If that time is over then users cannot access data file.

C. Algorithm Used

Ciphertext-Policy Attribute-based Encryption

The functionality and security model of CP-ABE believe that cloud server does not conduct the access control management. This type of schemes allow the user to query any ciphertext, but user is capable to decrypt the ciphertext if and only if his attribute set satisfies the AP of the file. A CP-ABE consists of the following

Setup**.** It takes a security parameter λ and the attribute universe description U as the input, and outputs a master key MK, and a public parameter PK.

Key Generation: It takes the master key MK and a set of attributes as the input, and outputs the security key SK associated with the input attribute set.

Encryption:It takes the public parameter PK, a message M, and an APT over some attributes as the input. It outputs the ciphertext CT.

Decryption:It takes the security key SK, and the ciphertext CT as the input, and outputs either a message M or the distinguished symbol $\perp$.

IV. Result And Discussions

D. Experimental Setup

I. All the experimental cases are implemented in Java in congestion with Netbeans tools and MySql as backend, algorithms and strategies, and the competing classification approach along with various feature extraction technique, and run in environment with System having configuration of Intel Core i5-6200U, 2.30 GHz Windows 10 (64 bit) machine with 8GB of RAM

E. Result Analysis

Table1 shows the precision and recall values for video retrieval with combination of OCR and ASR (Hybrid).Our proposed approach can do some improvement to existing approach by doing combination of OCR and ASR. As the value of precision and recall of Figure 2 For personalized video results sequence should change according to that user query interest.

Table 1. System measure analysis for multiple search query

Search Query / **Measures**	**Q1**	**Q2**	**Q3**
Precision	0.91	0.87	0.85
Recall	0.87	0.81	0.79
F-measure	0.87	0.84	0.84

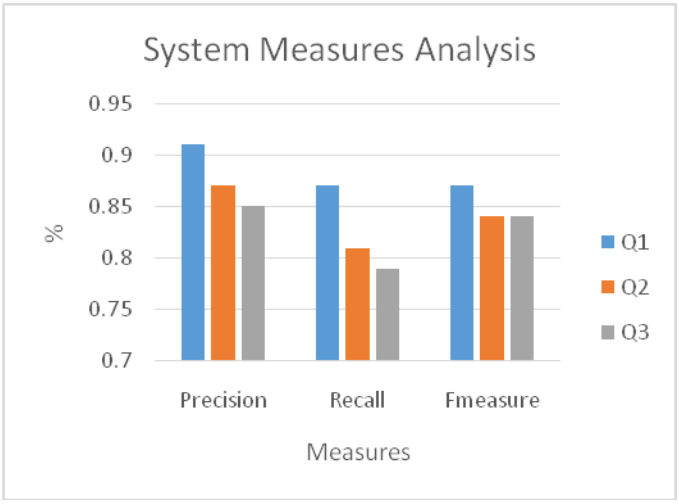

Fig. 2 System measure comparison for hybrid (OCR and ASR) algorithm

V. Conclusion

Many recent challenges have appeared withthe fast growth of adaptable cloud services. One of the most significant problems is how to securely delete the outsourced data stored in the cloud severs. In order to solve the problems by implementing flexible fine-grained access control during the authorization period and

time-controllable self-destruction after expiration to the shared and outsourced data in cloud computing, another challenge is to parallelly achieve both flexible timed release and fine granularity with less overhead, which was not analyzed in existing system. Here we proposed a data self-destructing system which is able to attain the time specified ciphertext. and a revocable outsourcing computation into Attribute based encryption, timed-release encryption to the architecture of ciphertext policy attribute-based encryption is introduced to overcome issue There is No secure channel or user authentication is required during key-update between user and

cloud, data owner have ability to flexibly grant the access privilege (AP) to different users at different time, according to a well-defined AP over attributes and release time. Our system preserve theconfidentiality of time-sensitive data

References

[1]. Jin Li, Jingwei Li, Xiaofeng Chen, ChunfuJia, and Wenjing Lou, "Identity-Based Encryption with Outsourced Revocation in Cloud Computing", in IEEE transactions on computers, vol. 64, no. 2, february 2015.
[2]. W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation," In Advances in Cryptology (CRYPTO98). New York, NY, USA:Springer, 1998, pp. 137-152.
[3]. A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proc. 15thACMConf. Comput. Commun.Security (CCS08), 2008, pp. 417-426.
[4]. D. Boneh and M. Franklin, "Identity-based encryption from the Weilpairing," in Advances in Cryptology (CRYPTO '01), J. Kilian, Ed.Berlin, Germany: Springer, 2001, vol. 2139, pp. 213-229.
[5]. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology (EUROCRYPT'05), R. Cramer, Ed. Berlin, Germany: Springer, 2005, vol. 3494, pp. 557-557.
[6]. J. Li, C. Jia, J. Li, and X. Chen, "Outsourcing encryption of attribute based encryption with mapreduce," in Information and Communications Security. Berlin, Heidelberg: Springer, 2012, vol. 7618, pp. 191-201.
[7]. B. Zhang, J. Wang, K. Ren, and C. Wang, "Privacy-assured Trans. Emerging Topics Comput., vol. 1, no. 1, p. 166-177, Jul. Dec. 2013 outsourcing of image reconstruction service in cloud," IEEE.
[8]. J. Li, X. Chen, J. Li, C. Jia, J. Ma, and W. Lou, "Fine-grained access control system based on outsourced attribute-based encryption," in Proc. 18th Eur. Symp. Res. Comput. Security (ESORICS), 2013,pp. 592-609.
[9]. R. Canetti, S. Halevi, and J. Katz, "A forward-secure publickeyEncryption scheme," in Advances in Cryptology (EUROCRYPT' 03), E. Biham, Ed. Berlin, Germany: Springer, 2003, vol. 2656,pp. 646-646.
[10]. S. G. Akl and P. D. Taylor, "Cryptographic Solution to a Problem of Access Control in a Hierarchy," ACM Transactions on Computer Systems (TOCS), vol. 1, no. 3, pp. 239–248, 1983.
[11]. R. S. Sandhu, "Cryptographic Implementation of a Tree Hierarchy for Access Control," Information Processing Letters, vol. 27, no. 2, pp. 95–98, 1988.
[12]. J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," in Proceedings of ACM Workshop on Cloud Computing Security (CCSW '09). ACM, 2009, pp. 103–114.
[13]. D. Boneh and M. K. Franklin, "Identity-Based Encryption from the Weil Pairing," in Proceedings of Advances in Cryptology – CRYPTO '01, ser. LNCS, vol. 2139. Springer, 2001, pp. 213–229.