ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

Time-Sensitive Data Access Management in Cloud by Combining Time and Attribute Factors

Rakshitha B Y[1] Ramya M[2] , Prof.Geetha Megharaj[3], Dr K.S Jagadeesh Gowda[4]

UG students, Department of CSE, Sri Krishna Institute of Technology, Bengaluru, India[1,2]

Associate Professor, Department of CSE, Sri Krishna Institute of Technology, Bengaluru, India [3]

Professor, Department of CSE, Sri Krishna Institute of Technology, Bengaluru, India [4]

ABSTRACT: The new pattern of outsourcing to the cloud is a two-edged sword. One side it allows data owner to upload their data and it provides easier way to share the data. Another side, it brings the new problems analysis on privacy and security for the data shared. To protect the private or personal data this confidential on the cloud, there is no honest cloud service provider. Until now there were no well-organised schemes that provide the fine-grained data access control with the time-sensitive data control. In this paper, we mainly combine the timed-release encryption with CP-ABE (Ciphertext Policy Attribute Based Encryption). Extensive security and performance analysis is proposed in well-organised way and the security of data is satisfied upon the requirements for storing the time-sensitive data on the cloud.

KEYWORDS: Time-Sensitive, Ciphertext-Policy, fine-grained

I. INTRODUCTION

Cloud computing is an information technology (IT) pattern that enables ubiquitous access to shared pools of configurable system resources and higher-level services that can be rapidly provisioned with minimal management effort, often over the Internet. Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a public utility.

Cloud storage factor has notable advantages on both convenient data sharing and costless sharing. However, this new pattern of data storage brings about new problems about data confidentiality protection and privacy. Data are no longer in data owner's security, and cannot trust the cloud server to conduct honest data access. Therefore, the honest data access problem has become a demanding issue in cloud storage. There are number of works on privacy containing data sharing in cloud based on various cryptographic methods are mainly based on CP-ABE, since they can guaranteed data owner fine-grained and flexible access control of data. However, these schemes determine user's access privilege only based attributes without any other critical aspects, such as the time factor. Now a day, the time factor usually plays an crucial role in dealing with time sensitive data. When uploading time-sensitive data to the cloud, the data owner may want different users to access the content after different time.

However, the best of our knowledge, existing CP-ABE based. Schemes can't help such prerequisite.

The principle commitments for this paper can be summarized as follows.

1) This paper aims that combined effect of time and attribute factors together .This paper deals with the architecture for the system proposed. The access to data control for shared data in cloud by timed-released.

2) We configure a viable constructing model to figure the access data control issue, in which we update an element (The Central Authority, CA) which will be answerable for those timed-release capacity. Furthermore distributing attribute-associated private keys, CA needs to eventually publish the keys. Time-related tokens should discharge entry

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

privileges. Such constructing model involves less amount of cost. Expense will provide our required right control scheme to work efficient.
3) For our Architecture, this is no need for secure tunnel between CA and data owner, this reduces the pressure on data owner

II. RELATED WORKS

The work in **[1]** includes cloud registering, which is viewed as a guaranteeing registering standard. An ever-increasing amount individuals store their delicate data information on the cloud. However, it is an incredible challenge for information security in gaining entrance to the touchy information on the cloud. In this paper, a control scheme, termed LTS-ACCESS, which accomplishes Lightweight, Time-specific also secure. Information right control for resource-limited units clinched alongside cloud stockpiling. Our LTS-ACCESS at the same time revels in those taking after properties:.
i) Steady span of the unscrambled keys, furthermore easier calculation. Cosset since the agent very nearly all of the unscrambling expense of the. Unscrambling administration provider.
ii) Time-specific, that delicate information. Manager might define a period interval, Therefore a collector can do unscramble. Those Ciphertext When it may be gained and a period moment magic need.
iii) Provably secure, the recommended plan may be. Provably secure under the specific security model. Completely, hypothetical in the execution assessment demonstrated. Also effectiveness from claiming our recommended LTS-ACCESS.

The work in **[2]** includes information gathering is a purpose in cloud capacity. In this paper, an hint at how should data be securely efficiently, also flexibly. Allotment information with others previously, cloud capacity. the portray new public-key cryptosystems that generate constant-size ciphertext that productive assignment from claiming unscrambling privileges for setting from claiming ciphertext need aid could be allowed. The variety will be at particular case might be set from claiming mystery keys. Furthermore settle on them similarly as conservative as a key, be that as including the force of every one of keys continuously. In other words, those mystery ways holder could arrival a constant-size aggravator enter to adaptable decisions about ciphertext set in cloud storage, yet the different encrypted files outside the situated stay private. This conservative key could a chance to be sent will others alternately be put away clinched alongside a card with thick, as constrained secure capacity. The formal security investigates about our schemes in the standard model. Likewise, portray other provision about the schemes.

The work in **[3]** includes a small percentage of the best complex issues on abstracts outsourcing data need aid from organization for allocating technique Ciphertext-policy attribute-based encryption will be a unable cryptographic band-aid on these issues to enforce confirmation power to an abstracts purchaser for outsourced information. However, those botheration from claiming those attribute-based encryption, previously an outsourced architectonics introduces a few tests with thoughtfulness regarding those perspective and client disavowal. In this paper, an confirmation power mechanical assembly provision ciphertext-policy attribute-based encryption to fulfil confirmation power conduct technique with unable part. The flying confirmation power can make refined toward bi-fold encryption mechanical assembly, which takes point of the attribute-based encryption. Furthermore, the cautious way organization clinched alongside commemoration angle aggregation. The validation will manage the suggested mechanical assembly will profoundly manage those outsourced information. Those test after-effects publish that those recommended course of action has the ability to the framework provided in the architecture.

The work in **[4]** includes consideration on the problem of sending messages into the future, commonly known as timed-release cryptography. Existing Schemes for this task either solve the relative time problem with uncontrollable, fine-grained release time (time-lock puzzle approach) or do not provide anonymous to senders and/or receivers and are not scalable (server based approach). Using a bilinear pairing on any Gap Diffie-Hellman group, the problem is solved by giving scalable, server-passive and user-anonymous timed release public-key encryption schemes allowing precise absolute release time specifications. Unlike the existing server-based schemes, the trusted time server in the scheme is completely passive — no interaction between it and the sender or receiver is needed; it is even not aware of the existence of a user, thus assuring the privacy of a message and the anonymity of both its sender and

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

receiver. Besides, our scheme also has a number of desirable properties including a single form of update for all users, self-authenticated time-bound key updates, and key insulation, making it a scalable and appealing solution. It could also be easily generalized to a more general policy lock mechanism.

The work in **[5]** includes the way of encryption supporting fairness test (referred as PKE-ET) gives the ability about testing the proportionality between two messages encrypted under distinctive funded keys. Ciphertext-Policy Attribute-based encryption (CP-ABE) will be a guaranteeing primitive should accomplish versant also secure information imparting in the cloud registering eventually Tom's perusing giving work to adaptable one-to-many encryption. In this paper, firstly instate the idea from claiming CP-ABE with correspondence test (CP-ABE-ET) toward joining those notions about PKE-ET also CP-ABE. Utilizing ABE-ET primitive, the recipient can represent a cloud server, which should perform a proportionality test between two messages, which would encrypted under separate get arrangements. Throughout the delegated comparability test, those cloud server may be unabated will get any learning of the message encrypted under possibly entry approach. The CP-ABE plan utilizing the bilinear matching combining with Vi_ete's formulas, which provides the security verification of the plan in the standard model.

III. SYSTEM ARCHITECTURE

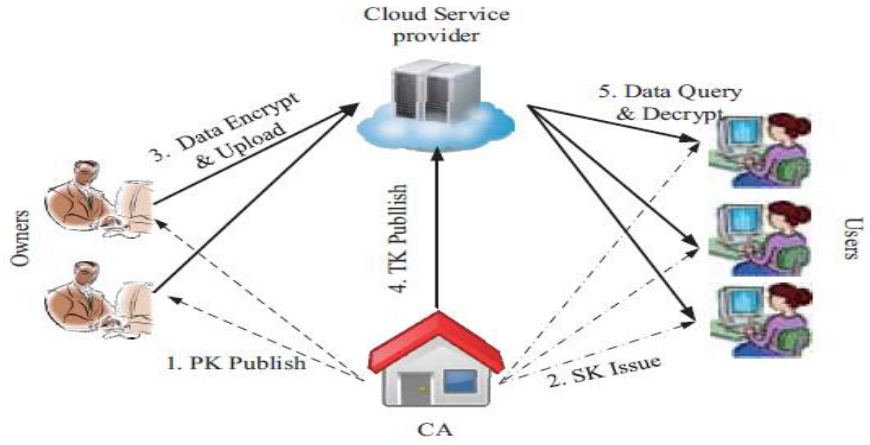

Fig 3.1: Architecture

As depicted in Fig. 3.1, the system consists of the following elements: cloud service provider (cloud), a central authority (CA), several data owners (owner), and many data service receiver (user).

• **Cloud service provider (cloud)** includes the manager of the cloud and cloud servers. The cloud stores a collection of data from owners, accepts download request from any users, as well as helps owners and users conduct onerous computations.

• **The central authority (CA)** is responsible to manage the security problem of the whole system: It publishes system options and distributes private keys related to specific attributes for each user. In addition, it acts as a time agent to publish the time-related secret (denoted as time token, TK) at each pre-defined time (This can be simplified as a periodic operation).

• **The data owner (owner)** decides the access policy based on attributes and release time, and then encrypts the data under the policy before uploading it.

• **The data consumer (user)** is assigned a private key from CA. The query from the user can be any ciphertext stored in the cloud, but is able to decrypt it only if user satisfies both of the following constraints:

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

1) User must possess the specified attributes and the access control will be given.
2) The current access time should be later than the corresponding release time.

The functionalities of the elements of the architecture

➢ **Data Owner:**

- Data owner should register
- Data owner can login only after activation by admin
- Data owner should get one time upload key before uploading any file
- Data owner should decrypt and download the upload key valid for one session
- Data owner can upload file to cloud by using the onetime upload key & attribute
- Data owner can logout

➢ **Data User:**

- Data user should register
- Data user can login only after activation of the account by admin
- Data user can search cloud files
- Data user can request for the file access, with open and close time
- Data user gets time key in the registered email account
- Data user can download the file by using One Time Key, Time Key, and OTP
- Data user cannot download the file once the time is expired
- Data user can logout

➢ **CA:**

- CA can login
- CA can view the user file access request and issue secret key
- CA can logout

➢ **Admin:**

- Admin can login
- Admin activates data owner & data user
- Admin provides one time upload key to data owner
- Admin can view all the files uploaded to cloud
- Admin can view all the time sensitive files uploaded to cloud
- Admin can send One Time Key, Time Key, and OTP to user for file access
- Admin can logout

IV. CONCLUSION

This paper aims at fine-grained entry control for time-sensitive information to cloud stockpiling. One test is with at the same time attain adaptable timed discharge for fine granularity with lightweight overhead, which may be not furnished On related fill in. In this paper, we recommend an plan on attain this objective. Our plan seamlessly incorporates the idea about timed-release encryption of the construction modelling for ciphertext-policy attribute-based encryption. With a suit of shield from claiming suggested mechanisms, this plan gives information managers with those proficience should flexibly arrival those entry benefit on different clients In separate time, as stated by a well-defined right approach through qualities that discharge the long run. Those dissection demonstrates that our plan camwood protect those secrecy from claiming time-sensitive data, with an lightweight overhead for both ca and information owners, consequently great suits the useful vast scale right control framework to cloud stockpiling.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 7, Special Issue 6, May 2018*

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

REFERENCES

[1] S. Yu, C. Wang, "Achieving secure, scalable, and fine-grained data access control in cloud computing", in Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS '10), 2010.
[2] Qiang Wang, Li Peng, Hu Xiong, Jianfei Sun and Zhiguang Qin, "Ciphertext-Policy Attribute-based Encryption with Delegated Equality Test in Cloud Computing", in Proceedings of the 28th IEEE Symposium on Security and Privacy (S&P2007), pp. 321–334, IEEE, 2007.
[3] J. Hur, D.K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems", in IEEE Transactions On Parallel and Distributed Systems, Vol. 22, No. 7, July 2011
[4] M. Li, S. Yu, "Scalable and secure sharing of personal health records in cloud computing using Attribute-Based Encryption".IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 1, pp. 131–143, 2013.
[5] C.K. Chu, S.S.M. Chow, "Key-aggregate cryptosystem for scalable data sharing in cloud storage", in IEEE Transactions On Parallel and Distributed Systems, Vol. 25, No. 2, February 2014.
[6]Yanchao Wang, Fenghua Li, Ben Niu and RongnaXie,"Achieving Lightweight, Time-Specific and SecureAccess Control in Cloud Storage" in2016 International Conference on Computing, Networking and Communications, Cloud Computing and Big Data.
[7] K. G. Paterson and E. A. Quaglia, "Time-specific encryption," inSecurity and Cryptography for Networks. Springer, 2010, pp. 1–16.