RESEARCHERID
THOMSON REUTERS

[Priyanka, 5(7): July 2018]
DOI- 10.5281/zenodo.1305952

ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

ENHANCING SECURITY AND EFFICIENCY OF KEY MANAGEMENT IN CLOUD DATA SHARING SYSTEM

Priyanka[*1] & Ch.Ramesh[2]

[*1]M. Tech Student, Department of CSE, G. Narayanamma Institute of Technology and Science (GNITS), Shaikpet, Hyderabad, India

[2]Assistant Professor, Department of CSE, G. Narayanamma Institute of Technology and Science (GNITS), Shaikpet, Hyderabad, India

ABSTRACT

The safe data sharing in cloud, cipher text policy attribute based encryption is promising as data owner having full control over access policy of shared data. Together with the growth of mobile applications, mobile cloud services have been introduced as a potential trend in cloud computing. Existing research work hardly notices that mobile front-end devices, such as smart phones, are far more vulnerable than servers with respect to privacy protection. Thus, the vulnerability in private key protection may easily lead to the exposure of keys to unauthorized users. In addition, current ABE key management schemes also require much bilinear pairing calculation, exponentiation and multiplication, especially in the decryption step. The resulting run time may be horribly unacceptable. In this paper, we propose a novel collaborative key management protocol in ciphertext policy attribute-based encryption (CKM-CP-ABE) aiming to enhance security and efficiency of key management in cloud data sharing system.

Keywords*: Cloud, Key management, Encryption and decryption, Bilinear Pairing.*

I. INTRODUCTION

Cloud safety is one of the main problems every day with the boom in today's generation. Cloud service vendors deliver us the power in one of the 3 bureaucracy SaaS. Paas, IaaS. Every provider supplied by way of cloud has its very own advantages. One of the critical aspects focusing inside the cloud computing era the price of facts sharing but at the same time protection warranty is also the essential purpose to be completed. Clouds carry out a vast range of benefits along with, computing resources, commercial financial savings, Flexibility. However, privateness and safety issues are uncovered to be the primary issue.

Therefore, facts protection and privateness are the most vital concern in cloud computing. Cryptography inside the cloud offers encryption techniques to comfy records in an effort to be used or stored inside the cloud. It lets in customers too conveniently and securely accesses shared cloud services, as any statistics this is saved in cloud garage is included with encryption. Cryptography techniques in the cloud computing protect touchy records with out delaying data trade. In security enforcement of records machine, an access manipulate is one of maximum typically used approach. Access manipulate is a coverage that allows, rejects or confines get entry to the assets in a computing environment. It additionally video display units and facts all attempts made to get right of entry to a gadget. It is a mechanism which is very tons essential for protection in computer protection. Accordingly, how to effectively and securely share consumer facts is one of the hardest challenges inside the scenario of cloud computing. This proposed work revised on Attribute-Based Encryption techniques which have been advanced thus far for attaining comfy information sharing in cloud computing.

Cloud computing is an alternative to records technology due to its useful resource-sharing and occasional-maintenance characteristics. With the recent adoption and diffusion of the facts sharing paradigm in allotted structures inclusive of on-line social networks or cloud computing, there were increasing needs and concerns for disbursed information security. As people enjoy the advantages of these new technology and offerings, their

concerns approximately facts security and get entry to manipulate also stand up. People would like to make their sensitive or non-public information simplest reachable to the authorized people with credentials they designated. There are diverse different issues inclusive of risks of privacy publicity, scalability in key control, flexible access and green person revocation. To obtain excellent grained and scalable information get admission to manage for any records saved in semi trusted servers, leverage attribute based encryption (ABE) strategies is a promising cryptographic method to encrypt document. ABE is anticipated as a crucial tool for addressing the trouble of secure and first-class-grained information sharing and access control. In an ABE system, a consumer is diagnosed with the aid of a fixed of attributes.

CP-ABE has end up to be a critical encryption generation to address the venture of secure data sharing. In a CP-ABE, person's secret key is defined by means of an attribute set, and ciphertext is associated with an get admission to shape. Data Owner (DO) is allowed to determine get entry to shape over the universe of attributes. A person can capable of decrypt a given encrypted text handiest if his/her attribute collection set suits the get entry to coverage over the ciphertext. Employing a CP-ABE gadget at once into a cloud utility which could yield some open issues; firstly, all secret keys of users need to be issued with the aid of an entirely relied on key authority (KA). This reasons a protection threat this is referred to as key escrow trouble. By knowing the name of the game key of a consumer, the KA can able to decrypt the complete user's cipher texts which is in total in opposition to the will of the consumer; secondly, the expressiveness of attribute set is any other difficulty. The present CP-ABE schemes can handiest outline binary state over characteristic, as an instance, 1 for pleasing and 0 for no longer-gratifying, but now not dealing with the arbitrary-realm attribute.

II. RELATED WORK

Key trade conventions rely upon a by and large trusted key age focus (KGC) to pick session keys and dispatching session keys to all correspondence elements furtively. Regularly, KGC encodes session keys under another secret key imparted to every element all through enrollment. S. Rafaeli, & D. Hutchison have optimized dynamic multicast key distribution scheme with MDS codes the usage of PFMH tree. The computation complexity of key distribution is substantially decreased by way of employing erasure decoding of MDS codes rather than extra high priced encryption and decryption computations. The MDS codes was combined with PFMH bushes and overall performance of distribution time and key restoration time turned into evaluated, this scheme offers much decrease computation complexity at the same time as keeping low and balanced communication complexity and garage complexity for dynamic group key distribution. This scheme is thus sensible for plenty packages in diverse broadcast capable networks which include Internet and wi-fi networks.

C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou proposed a privacy-keeping public auditing system for statistics storage safety in Cloud Computing. They used the homomorphic direct authenticator and irregular covering to ensure that the TPA won't not look into any learning roughly the data content put away on the cloud server all through the green reviewing system, which no longer least complex dispenses with the weight of cloud client from the monotonous and most likely extravagant examining challenge, however also reduces the clients' stress in their outsourced records spillage. Considering TPA may additionally simultaneously take care of multiple audit sessions from special users for his or her outsourced facts files, they in addition amplify their privateness-retaining public auditing protocol into a multi-person placing, where the TPA can perform more than one auditing obligations in a batch way for better performance. Extensive analysis indicates that their schemes are provably secure and incredibly green.

H. Hong, Z. Sun mixed the benefit of key-insulation mechanism with ABE and proposed a excessive efficient key-insulated ABE algorithm without pairings (KI-ABE-WP). During the going for walks of algorithms in our scheme, users and AA needn’t run any bilinear pairing operations. The high performance and proved safety make their scheme greater appropriate for records sharing in community structures, especially people with limited computing potential which includes wireless sensor networks, cellular verbal exchange system, and many others.

Q. Liu, G. Wang, and J. Wu addressed an essential issue of comfortable statistics sharing on untrusted storage. Toward offering a fullfledged cryptographic basis for secure records sharing on untrusted storage, they proposed 3 protection-enhancing solutions for ABE: The first enhancement they made is to offer green person revocation in ABE. In this thesis, they especially had taken into consideration practical utility scenarios wherein semi-trustable proxy servers are available. With this assumption they uniquely mixed the proxy re-encryption technique with ABE and enabled the authority to delegate maximum exhausting duties to proxy servers. Such an enhancement places minimum load on authority while revoking customers. Their proposed scheme is provably secure in opposition to selected cipher textual content assaults. In their second enhancement to ABE, they addressed key abuse attacks and proposed an abuse free KP-ABE (AFKP-ABE) scheme.

III. FRAMEWORK

A. Overview of Proposed System

The proposed model includes 5 implementation modules;

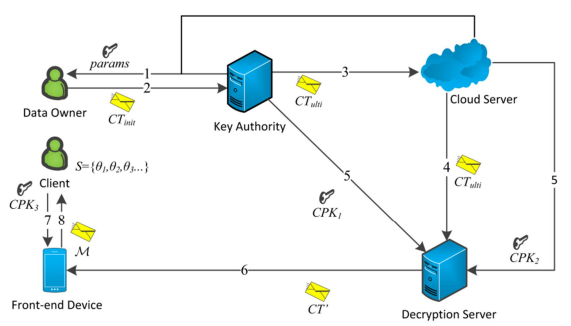

Fig1. Proposed CKM-CP-ABE model

Client:

A Client (CL) is a consumer who intends to get right of entry to information in cloud storage thru front-quit devices. With the capability trend of mobile cloud services, mobile devices are most people of front-give up deices. If the CL's characteristic set satisfies an access coverage related to ciphertext, the CL might be allowed to collect plaintext. We count on that maximum mobile devices are overall performance-constrained, so CLs may be in hazard of struggling key publicity.

Key Authority:

The key authority (KA) is a important issue in the machine. The KA is answerable for most calculating duties, including key technology, key update, and so on. We anticipate that the KA is semi-trusted in our system, meaning it is curious about the price of plaintext however has no purpose of tampering with it.

Cloud Server:

A cloud server (CS) is responsible for cloud garage control. All the records to be shared are in the control of the CS. We expect that any CS is semi-depended on.

Decryption Server:

The decryption server (DS) has powerful computing skills. It undertakes and isolates the most, however no longer all project of decryption. We assume that the DS is semi-trusted and the DS get right of entry to channel is insecure, due to the fact it is enough for CKM-CP-ABE to assure statistics protection.

Data Owner:

An information owner (DO) is an authorized user inside the machine that possesses information to be uploaded. DOs outline their own explicit access policies so that only applicable CLs are granted permission to obtain plaintext.

B. Working of Proposed System

In the working, all the implementation modules are concerned in information sharing does now not collude with each other to get admission to data illegally; in any other case the scheme could be unavailable and meaningless. In our model, attributes are authenticated with the aid of the KA. All granted attributes are represented through a set of random elements blanketed in public parameters, which is generated with the aid of the KA in collaboration with a CS. Let params be public parameters. When a DO intends to share data, it encrypts the records the usage of params sent to shape the preliminary ciphertext CT_{init} and uploads it to the KA. The KA re-encrypts the initial ciphertext to form the ultimate ciphertext CT_{ulti}, which is sent to and stored in a CS. According to the CL's attribute set S= {θ_1, θ_2, θ_3, …}, the key management protocol helps to simultaneously and secretly generate three different components of the private key, namely, CPK_1 , CPK_2 and CPK_3 , each of which is kept by one of KA, CS or CL. Once asked for data stored in the cloud, the DS receives CPK_1 and CPK_2 to transform CT_{ulti} to CT′. Eventually, the CL extracts the plaintext *M* from CT′ by its CPK_3.

IV. CONCLUSION

In this paper, we suggest a novel collaborative key management protocol to beautify each safety and performance of key control in ciphertext policy attribute-based encryption for cloud statistics sharing system. Distributed key technology, difficulty and storage of private keys are found out without including any extra bodily infrastructure. We introduce attribute companies to construct a private key update set of rules for pleasant-grained and instantaneous attribute revocation. The proposed collaborative mechanism flawlessly addresses not handiest key escrow trouble but additionally a worse hassle referred to as key exposure that previous research hardly noticed. Meanwhile it helps to optimize clients' consumer revel in view that most effective a small amount of duty is taken with the aid of them for decryption.

REFERENCES

1. *Guofeng Lin, Hanshu Hong, and Zhixin Sun, "A Collaborative Key Management Protocol in Ciphertext Policy Attribute-Based Encryption for Cloud Data Sharing", DOI 10.1109/ACCESS.2017.2707126, IEEE Access*
2. *S. Rafaeli, and D. Hutchison, "A survey of key management for secure group communication," ACM Computing Survey, vol. 35, no. 3, pp. 309-329, 2003.*
3. *C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," IEEE Trans. Comput., vol. 62, no. 2, pp. 362-375, 2013*
4. *H. Hong, Z. Sun, "High efficient key-insulated attribute based encryption scheme without bilinear pairing operation," SpringerPlus, vol. 5, no. 1, pp. 131, 2016.*
5. *Q. Liu, G. Wang, and J. Wu, "Time-based proxy re-encryption scheme for secure data sharing in cloud environment," Information Sciences, vol. 258, pp. 355-370, 2014*
6. *C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," IEEE Trans. Comput., vol. 62, no. 2, pp. 362-375, 2013.*
7. *Q. Wu, "A generic construction of ciphertext-policy attribute-based encryption supporting attribute revocation," China Commun., vol. 11, no. 13, pp. 93-100, 2014.*
8. *B. Waters, "Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization," in Proc. Public Key Cryptography, 2011, pp. 53-70.*
9. *M. Green, S. Hohnberger, and B. Waters, "Outsourcing the decryption of ABE ciphertext," in Proc. USENIX Secur. Symp., 2011, pp. 34.*
10. *D. Pletea, S. Sedghi, M. Veeningen, and M. Petkovic, "Secure distributed key generation in attribute based encryption systems," in Proc. ICITST, 2015, pp. 103-10*