A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing

Sudipto Palit[1] Dr. Tripti Arjariy[2]
[1,2]Department of Computer Science & Engineering
[1,2]Rajiv Gandhi Proudyogiki Vishwavidhyalaya, India

Abstract— In mobile cloud computing the data security problem are becomes more grievous and intercept in the development of mobile clouds. In the mobile clouds there many research are done to improve the mobile cloud security. But many clouds are not supporting to the mobile services since mobile devices has limited power and computing resources. To find the solutions to mobile cloud applications with low computational overhead is important task. In this research paper, we proposed technique to solve this issues for mobile cloud computing. The normal cloud environment has an access control technology, but the proposed system changes the access control tree to use easily cloud environment with mobiles cloud. We discuss the proposed technique for mobile cloud computing. Attribute-based encryption (ABE) system is used for cloud storage security when multiple users are read the same file which is stored on the mobile cloud. For the personal storage system, we developed the modified cipher text-policy attribute based encryption system using flexible and expressive access policy in public domains. Our scheme supports multi-authority scenario, in which the authorities work independently without an authentication center. To decrease the user revocation cost, it also introduce the attribute description fields for implementing the efficient lazy revocation, it is an important issue in program based CP-ABE system. We try improving performance of system with respect to time.

Key words: ABE, Cloude, Encryption, Decryption, Multi-Authority

I. INTRODUCTION

Now a day's cloud computing is widely use. More than 50% of IT companies have moved their Business to the cloud. Sharing of data over the cloud is the new trend that is being set on. The data generated on a day to day life is increasing and to store that all of the data in traditional hardware is not possible because of limited storage capacity. Therefore, transferring the data to the cloud is a necessity where the user can get unlimited storage. Security of that data over is the next big concern for most of us. After uploading the data to the cloud use loses its control over that data [1]. In mobile devices, personal data files are sensitive. In many mobile clouds data owners are given permission to access the files in publically or in private mode. The security of personal data is the important point all mobile data owners. Many times all cloud users are upload their data on cloud and leaving their data on cloud where monitoring over that data is out of their control, the cloud service provider can also spy on the personal data of the users. When someone has to share data over the data they have to share the password to each and every user for accessing the encrypted data which is cumbersome. Therefore, to solve this problem mobile data are encrypted before uploading on the cloud which can be safe from everyone. Now the data encryption part brings.

Cipher text-policy attribute based encryption (CP-ABE) [2] is a public-key cryptography primitive that are proposed to determine the correct issue of fine-grained get to control on shared information in one-to-numerous correspondences. In CP-ABE, every client is doled out an arrangement of traits which are installed into the client's mystery key. An open key segment is characterized for every client property. While encoding the message, the scrambled picks an entrance structure on characteristics, and scrambles the message under the entrance structure by means of scrambling with the comparing open key parts. Clients can decode a figure content if and just if their properties fulfil the figure content access structure. People in general key and figure content sizes in CP-ABE are only straight to the quantity of characteristics and the multifaceted nature of the entrance structure, which is free to the quantity of clients. In addition, CP-ABE is impervious to conspiracy assaults from unapproved clients. All these pleasant properties make CP-ABE greatly reasonable for fine-grained information get to control on untrusted capacity.

Infrastructure and operations (I&O) leaders should plan for cloud services that are made up of orchestrated technology and/or application elements, not just the individual technology components. These cloud services could be varied and be sourced from internal IT teams, third parties providing private cloud services or public cloud services. Although there is an increase in the adoption of public cloud services, the future for many organizations will involve hybrid cloud deployments that increase complexity and the need to strategically handle the delivery of a suite of cloud services — for example, infrastructure as a service (IaaS), platform as a service (PaaS) and SaaS from different providers. To give protection and upgrade security to cloud clients, there are many security proposition as of late. In any case, because of the dynamic system topology of portable systems the current security proposition displayed which could accomplish both of the secrecy and information get to control may not be reasonable in versatile distributed computing. In particular, the quality based encryption or multi-beneficiary encryption which is more reasonable for a static and little scale organize as opposed to for the portable system, which is commonly powerful and possibly included a huge number of versatile clients who could join or leave the system discretionarily. Also one client may have numerous property and on the other hand one traits might be controlled by numerous clients which makes the information proprietor hard to set up the correspondence between the clients and qualities. These perceptions propel us to propose a novel information benefit system in versatile distributed computing.

The remainder of the paper is organized as follows. In section II, we are discussing the related works of ABS and data sharing over cloud computing. In section III, discuss proposed work. In section IV, the results and analysis is presented. Finally in section V, the conclusion and future work is presented.

II. RELATED WORK

This section presents the review of previous methods precisely work. In this we discus all cryptography technique, CP-ABE schema.

A. Chandni Patel (2015)

In [1] author show a proposed security system for portable distributed computing. In this system the cryptographic techniques and also calculations are utilized for encryption and decoding of portable client information. This Framework guarantees the extra security and classification of client's touchy or huge information. This paper presents the plotting stream of proposed security structure. This proposed Security structure is for the reason to anchor and give protection and trustworthiness to client's classified information in Mobile Cloud Environment.

B. Shubham Chandugade (2017)

The main challenge faced by everyone is to share the data all over the world or at organizational level securely without giving away the important data to any exploiters. To overcome the challenges to share the data securely over the cloud and an efficient data encryption algorithm are used to encrypting data for sending data on the cloud. In this proposed they are using a combination of Attribute-Based Encryption and Byte Rotation Encryption Algorithm for encrypting the mobile data for sending on the cloud. It will help the user to securely store and share the data in encrypted form.

C. Junzuo Lai (2014)

In [3] they propose a lightweight information sharing arrangement (LDSS) for versatile circulated registering. It gets CP-ABE, in common cloud condition, anyway changes the structure of access control tree to make it proper for versatile cloud circumstances. LDSS uses external servers to perform better figuring for gaining than power tree change in CP-ABE from phones. The preliminary occurs show that time taken for encryption of record concerning number of attributes varies depending upon the amount of qualities.

D. Yu S (2010)

In [4] paper they center on a critical issue of characteristic denial which is bulky for CP-ABE plans. Specifically, we re-comprehend this testing issue by considering more reasonable situations in which semi-trustable on-line intermediary servers are accessible. When contrasted with existing plans, our proposed arrangement empowers the expert to disavow client traits with negligible exertion. We accomplish this by interestingly coordinating the strategy of intermediary re-encryption with CP-ABE, and empower the specialist to designate the greater part of relentless undertakings to intermediary servers. Formal examination demonstrates that our proposed plot is provably secure against picked figure content assaults. Likewise, we demonstrate that our procedure can likewise be material to the Key-Policy Attribute Based Encryption (KP-ABE) partner.

E. Kan Yang (2014)

In [5] paper, they propose a novel plan that empowering proficient access control with dynamic strategy refreshing for huge information in the cloud. We center on building up an outsourced approach refreshing strategy for ABE frameworks. Our technique can stay away from the transmission of encoded information and limit the calculation work of information proprietors, by making utilization of the already scrambled information with old access strategies. Additionally, they likewise outline arrangement refreshing calculations for various sorts of access strategies. The examination demonstrates that our plan is right, entire, secure and effective.

F. Jia W (2011)

In [6] paper, they plan a protected versatile client based information benefit system (SDSM) to give privacy and fine-grained get to control for information put away in the cloud. This component empowers the versatile clients to appreciate a safe outsourced information administrations at a limited security administration overhead. The center thought of SDSM is that SDSM outsources the information as well as the security administration to the versatile cloud in a trust way. Our investigation demonstrates that the proposed instrument has numerous favorable circumstances over the current customary strategies, for example, bring down overhead and advantageous refresh, which could better provide food the prerequisites in portable distributed computing scenario.

G. I. Denisow (2015)

In [7] paper, ABE is reached out with dynamic characteristics. This enables credits to be added to a current private key. A server segment named Attribute Authority is presented. By utilizing these dynamic characteristics, it is currently conceivable to have the unscrambling rely upon information that change frequently, for example, area data of a cell phone. Two plans were produced that change over area information into usable ABE characteristics. To exhibit our outcomes, an Android application was actualized and assessed in a field test.

H. A. Sahai (2012)

In [8] they find that an exhaustive answer for our concern should at the same time take into consideration the renouncement of ABE private keys and in addition take into consideration the capacity to refresh figure writings to mirror the latest updates. In applications, such capacity might be with an untrusted substance and accordingly, they require that the figure content administration tasks should be possible without access to any touchy information. They characterize the issue of revocable stockpiling and give a completely secure development. Securing Newly Encrypted Data They consider the issue of guaranteeing that recently encoded information isn't decode table by a client's critical if that client's entrance has been denied. They give the principal technique for getting this disavowal property in a completely secure ABE conspire. They give another and less difficult way to deal with this issue has insignificant changes to standard ABE. We recognize and characterize a basic property called piecewise key age which offers ascend to proficient disavowal.

I. L. Touati (2015)

In this [9], they propose an answer which does not require additional substances like intermediaries to re-encode information after each entrance approach change. In addition, our answer does not infer latencies following access awards and renouncements. We contrast our answer and the bunch based CP-ABE characteristic administration method and we demonstrate that our answer beats existing rekeying/repudiation procedures as far as overhead.

J. S. Alshehri (2012)

In this [10] proposes the use of Cipher text-Policy Attribute-Based Encryption (CPABE) to encrypt EHRs in light of medicinal services suppliers' characteristics or qualifications, to unscramble EHRs, they should have the arrangement of traits required for appropriate access. The plan and utilization of a cloud-construct EHR framework situated in light of CP-ABE is persuaded and exhibited, alongside fundamental investigations to examine the adaptability and versatility of the proposed approach.

III. PROPOSED METHODOLOGY

In this section, we describe all function of our proposed work. In this work it has the four fundamental algorithms: Setup, Key Generation, Encryption and Decryption.

– Setup: The setup algorithm takes no input other than the implicit security parameter. It outputs the public parameters PK and a master key MK.
– Input: The attribute set A, the version attribute V.
– Output: The master key MK, the public key PK.

1) Construct a p-order bilinear group G0 of generator g and a bilinear mapping. e:$G_0 * G_0 = G_1$
2) Randomly choose a,bϵ $Z_p$and calculate $g^b, e(g,g)^a$
3) For each attribute ai in A, randomly choose $t_i \epsilon Z_p$, and calculate $X_i = g^t$
4) For V, randomly choose $t_v \epsilon Z_p$,, and calculate $X_v = g^t$
5) Return the master key MK and the public key PK, Wherein MK={a,b}, PK={ G0 , g , gb, $e(g,g)^a$, $\{Xi\}_{i=1}^k$, X_v}

A. Key Gen (MK,PK, L, ID):

The key generation algorithm takes as input the master key MK, public key PK, an identity ID and the attribute list L. It outputs a private key SKL for the attribute list L. Each authority manages its own attributes set and is responsible for key distribution to legal users (accessors). Once an authority authenticates identity of an accessor, it will process key generation which takes the master keys MK for a requested set of attributes as input and outputs user attribute components L for each attribute. All the attributes generated for the specific accessor are collected as secret key of the accessor SKL and sent back to the accessor secretly.

B. Encrypt (S, PK, P, M)

The encryption algorithm takes as input a revocation set S of identities, public parameters PK, the message m, and an access policy P over the universe of attributes. The algorithm will encrypt m and produce a cipher text CT such that any user with a key for an identity ID / ∈ S and the attribute list L satisfies the access policy can decrypt. Once the data owner gets public keys PK from authorities, he can execute encryption process in his own terminal. The algorithm takes from several authorities, message m for encryption, and an access policy P specified by the data owner as inputs. Then, the algorithm encrypts M to a cipher text and generates a public attribute component (abbreviated as) for each leaf node of P. The whole data tuple CT= {M'. policy P, S} of is the final cipher text tuple and is uploaded to cloud storage.

– Input: The symmetric key K, public key PK, access control tree T (including the left sub tree Ta, right sub tree Tv, and left sub tree has num leaf nodes).
– Output: The cipher text CT.

1) Randomly choose S ϵZp as the secret of T, and calculate CTk={gbS, K. e(g,g)aS }.
2) Get the value of the two children (namely Sa, Sv) of the root node according to the access control tree.
3) Calculate CTv={ $\{g^{Sv}, g^r, X_v^{Sv}\}$
4) Return CT={ CTk, CTa, CTv }.

C. Decrypt (CT, SKL, ID, S)

The decryption algorithm takes as input the cipher text CT that was generated for the revoked set S, as well as an identity and a private key SKL for the attribute list L. If the list L of attributes satisfies the access policy P and the ID / ∈ S then the algorithm will decrypt the cipher text and return a message M. An accessor receives CT from the cloud storage, finds out the minimal set of attributes S for decryption according to the policy, and then requests corresponding for attributes (AC1). Notice that the minimal attributes set Au is mapped to R1 rows of matrix. The rows set is labeled as Ix, where R1and ≤ R. According to sub matrix, the algorithm can compute values $\{\zeta_x \in \mathbb{Z}_n\}|_{x\in\{I_x\}}$, which has the relationship with the plaintext is computed by $D = D'/\tilde{e}(g_1, g_1)^s$.

IV. RESULTS & DISCUSSION

To evaluate the efficiency of the proposed solution, we conduct several experiments. The test of proposed work is done with LDSS and BSW. So in figure 1 shows the relationship between encryption time and the size of access control policy and figure 2 shows relationship between decryption time the size of access control policy.

The time needed for encryption and decryption is shown in 1 and Fig 2. As can be seen from both the overhead of encryption and decryption operations is proportional to the number of attributes in access control policy.

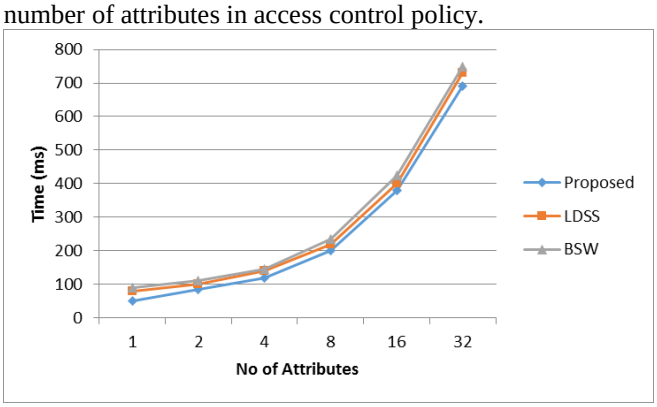

Fig. 1: Relationship between Encryption Time & the Size of Access Control Policy

In proposed technique, it takes a little less time. So we can say that our proposed system is more efficient that the existing techniques. Besides, the encryption and decryption time are close in all technique when the number of attributes rises to 32 in both schemes.

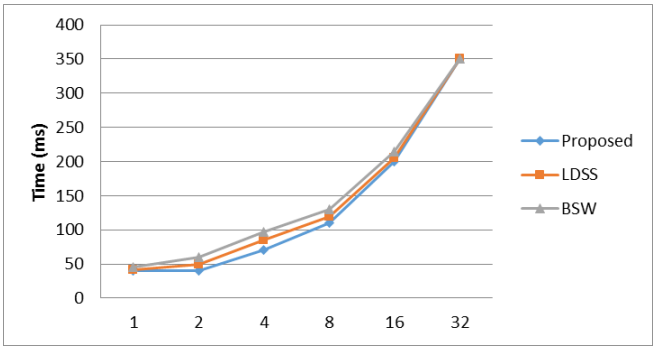

Fig. 2: Relationship between Decryption Time and the Size of Access Control Policy

V. CONCLUSION & FUTURE WORK

From last decade many authors studded on access control of clouds are based on attribute based encryption algorithm (ABE). In this paper we presenting the cloud computing cryptography and also number of recent methods which are studded for access control in cloud are based on attribute-based encryption algorithm (ABE). The issue of sharing the data in cloud computing securely is resolved. Data privacy can be maintained by combination of ABE and decryption. This indicates that the proposed system can be used to enhance privacy preservation in cloud services. It is deal with the secured mobile data sharing problem in flexible mobile cloud. The experimental results are prove that proposed work ensures security and data privacy in mobile cloud and also reduce time of processing as well. In the future work, we will design new approaches for all kind of data and try to share data on different cloud services.

REFERENCES

[1] Chandni Patel, SameerSingh Chauhan Bhavesh Pate, "A Data Security Framework for Mobile Cloud Computing", International Journal of Advanced Research in Computer and Communication EngineeringVol. 4, Issue 2, February 2015.
[2] Shubham Chandugade, Prachi More. "Survey on Lightweight Secured Data Sharing Scheme for cloud computing", International Research Journal of Engineering and Technology (IRJET)-ISSN: 2395-0056 Volume: 04 Issue: 10 Oct 2017
[3] Junzuo Lai, Robert H. Deng ,Yingjiu Li ,et al. Fully secure keypolicy attribute-based encryption with constant-size ciphertexts and fast decryption. In: Proceedings of the 9th ACM symposium on Information, Computer and Communications Security (ASIACCS), pp. 239-248, Jun. 2014.
[4] Yu S., Wang C., Ren K., et al. Attribute based data sharing with attribute revocation. in: Proceedings of the 5th International Symposium on Information, Computer and Communications Security (ASIACCS), New York, USA: ACM press pp. 261-270, 2010.
[5] Kan Yang, Xiaohua Jia, Kui Ren, Ruitao Xie, Liusheng Huang: Enabling efficient access control with dynamic policy updating for big data in the cloud. INFOCOM 2014, pp.2013-2021, 2014.
[6] Jia W, Zhu H, Cao Z, et al. SDSM: a secure data service mechanism in mobile cloud computing. in: Proceedings of 30th IEEE International Conference on Computer Communications. Shanghai, China: IEEE, pp. 1060-1065, 2011.
[7] Denisow, S. Zickau, F. Beierle, and A. K¨upper, "Dynamic location information in attribute-based encryption schemes," in Proceedings of the 9th International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST 2015). IEEE, 2015.
[8] Sahai, H. Seyalioglu, and B. Waters, "Dynamic credentials and ciphertext delegation for attribute-based encryption," in Advances in Cryptology–CRYPTO 2012. Springer, 2012.
[9] L. Touati and Y. Challal, "Efficient cp-abe attribute/key management for iot applications," in Computer and Information Technology (CIT), 2015 IEEE International Conference on. IEEE, 2015
[10] S. Alshehri, S. P. Radziszowski, and R. K. Raj, "Secure access for healthcare data in the cloud using ciphertext-policy attribute-based encryption," in Data Engineering Workshops (ICDEW), 2012 IEEE 28th International Conference on. IEEE, 2012.

