AN ATTRIBUTE BASED ENCRYPTION ALGORITHM FOR SECURITY IN MOBILE CLOUD COMPUTING APPLICATIONS

Sivani Ardhamala[1], Padmavathamma M[2]
[1]PG Student, Department of Computer Science, Sri Venkateshwara University Tirupati
[2]Professor, Department of Computer Science, Sri Venkateshwara University Tirupati

Abstract
With the notoriety of cloud computing, cell phones can store/recover individual information from anyplace whenever. Therefore, the information security issue in versatile cloud turns out to be increasingly serious and counteracts further advancement of portable cloud. There are significant examinations that have been led to improve the cloud security. In any case, a large portion of them are not pertinent for versatile cloud since cell phones just have restricted registering assets and power. Arrangements with low computational overhead are in incredible requirement for versatile cloud applications. In this paper, we propose a lightweight data sharing plan (LDSS) for portable cloud computing. It receives CP-ABE, an entrance control innovation utilized in typical cloud condition, however changes the structure of access control tree to make it reasonable for versatile cloud situations. LDSS moves an expansive segment of the computational serious access control tree change in CP-ABE from cell phones to outside intermediary servers. Besides, to decrease the client denial cost, it acquaints property depiction fields with actualize lethargic repudiation, which is a prickly issue in program-based CP-ABE frameworks. The exploratory outcomes demonstrate that LDSS can successfully decrease the overhead on the cell phone side when clients are sharing information in versatile cloud conditions.

Keywords: Cloud Computing, Information Security, Light weight information sharing plan.

I. INTRODUCTION

With the improvement of cloud computing and the ubiquity of savvy cell phones, individuals are bit by bit getting familiar with another period of information sharing model in which the information is put away on the cloud and the cell phones are utilized to store/recover the information from the cloud. Regularly, cell phones just have restricted storage room and figuring power. In actuality, the cloud has colossal measure of assets. In such a situation, to accomplish the tasteful execution, it is fundamental to utilize the assets given by the cloud specialist co-op (CSP) to store and share the information.

These days, different cloud versatile applications have been generally utilized. In these applications, individuals (information proprietors) can transfer their photographs, recordings, reports and different documents to the cloud and offer this information with other individuals (information clients) they like to share. CSPs likewise give information the executives usefulness to information proprietors. Since individual information documents are touchy, information proprietors are permitted to pick whether to make their information records open or must be imparted to explicit information clients. Plainly, information protection of the individual delicate information is a major worry for some information proprietors. The cutting edge benefit the executives/get to control instruments given by the CSP are either not requirements of information proprietors. In the first place, when individuals transfer their information documents onto the cloud, they are leaving the information in a spot where is out of their control, and the CSP may keep an eye on client information for its business advantages and additionally different reasons. Second, individuals need to send secret key to every datum client in the event that they just need to impart the scrambled information to specific clients, which is lumbering. To improve the benefit the board, the information proprietor can isolate information clients into various gatherings and send secret phrase to the gatherings which they need to share the information. Be that as it may, this methodology requires fine-grained get to control. In the two cases, secret phrase the executives are a major issue.

Clearly, to take care of the above issues, individual touchy information ought to be scrambled before transferred onto the cloud with the goal that the information is secure against the CSP. In any case, the information encryption brings new issues. The most effective method to give proficient access control instrument on ciphertext decoding with the goal that just the approved clients can get to the plaintext information is testing. Likewise, framework must offer information proprietors compelling client benefit the board capacity, so they can allow/repudiate information get to benefits effectively on the information clients. There have been considerable investigates on the issue of information get to command over ciphertext. In these examines, they have the accompanying regular suppositions. To begin with, the CSP is viewed as fair and inquisitive. Second, all the touchy information is encoded before transferred to the Cloud. Third, client approval on specific information is accomplished through encryption/unscrambling key dissemination. As a rule, we can partition these methodologies into four classifications: basic ciphertext get to control, progressive access control, get to control dependent on completely homomorphic encryption [1][2] and get to control dependent on trait-based encryption (ABE). Every one of these recommendations are intended for non-versatile cloud condition. They expend expansive measure of capacity and calculation assets, which are not accessible for cell phones. As indicated by the test results in [26], the fundamental ABE tasks take any longer time on cell phones than PC or personal computers. It is somewhere around multiple times longer to execute on an advanced mobile phone than a (PC). This implies that an encryption task which takes one minute on a PC will take about thirty minutes to complete on a cell phone. Moreover, current arrangements don't tackle the client benefit change issue great. Such an

activity could result in exceptionally high disavowal cost. This is not material for cell phones also. Plainly, there is no legitimate arrangement which can viably tackle the protected information sharing issue in versatile cloud. As the versatile cloud turns out to be increasingly prominent, giving an effective secure information sharing instrument in portable cloud is in dire need.

To address this issue, in this paper, we propose a Lightweight Data Sharing Scheme (LDSS) for portable cloud computing condition. The main contributions of LDSS are as follows:

(1) We design an algorithm called LDSS-CP-ABE based on Attribute-Based Encryption (ABE) method to offer efficient access control over ciphertext.

(2) We use proxy servers for encryption and decryption operations. In our approach, computationally intensive operations in ABE

are conducted on proxy servers, which greatly reduce the computational overhead on client-side mobile devices. Meanwhile, in LDSS-CP-ABE, in order to maintain data privacy, a version attribute is also added to the access structure. The decryption key format is modified so that it can be sent to the proxy servers in a secure way.

(3) We introduce lazy re-encryption and description field of attributes to reduce the revocation overhead when dealing with the user revocation problem.

(4) Finally, we implement a data sharing prototype framework based on LDSS. The experiments show that LDSS can greatly reduce the overhead on the client side, which only introduces a minimal additional cost on the server side. Such an approach is beneficial to implement a realistic data sharing security scheme on mobile devices. The results also show that LDSS has better performance compared to the existing ABE based access control schemes over ciphertext.

II RELATED WORK

Attribute-based fine-grained access control with efficient revocation in cloud storage systems

A cloud storage service allows data owner to outsource their data to the cloud and through which provide the data access to the users. Because the cloud server and the data owner are not in the same trust domain, the semi-trusted cloud server cannot be relied to enforce the access policy. To address this challenge, traditional methods usually require the data owner to encrypt the data and deliver decryption keys to authorized users. These methods, however, normally involve complicated key management and high overhead on data owner. In this paper, we design an access control framework for cloud storage systems that achieves fine-grained access control based on an adapted Ciphertext-Policy Attribute-based Encryption (CP-ABE) approach. In the proposed scheme, an efficient attribute revocation method is proposed to cope with the dynamic changes of users' access privileges in large-scale systems. The analysis shows that the proposed access control scheme is provably secure in the random oracle model and efficient to be applied into practice.

Achieving Usable and Privacy-assured Similarity Search over Outsourced Cloud Data

As the data produced by individuals and enterprises that need to be stored and utilized are rapidly increasing, data owners are motivated to outsource their local complex data management systems into the cloud for its great flexibility and economic savings. However, as sensitive cloud data may have to be encrypted before outsourcing, which obsoletes the traditional data utilization service based on plaintext keyword search, how to enable privacy-assured utilization mechanisms for outsourced cloud data is thus of paramount importance. Considering the large number of on-demand data users and huge amount of outsourced data files in cloud, the problem is particularly challenging, as it is extremely difficult to meet also the practical requirements of performance, system usability, and high-level user searching experiences. In this paper, we investigate the problem of secure and efficient similarity search over outsourced cloud data. Similarity search is a fundamental and powerful tool widely used in plaintext information retrieval, but has not been quite explored in the encrypted data domain. Our mechanism design first exploits a suppressing technique to build storage-efficient similarity keyword set from a given document collection, with edit distance as the similarity metric. Based on that, we then build a private trie-traverse searching index, and show it correctly achieves the defined similarity search functionality with constant search time complexity. We formally prove the privacy-preserving guarantee of the proposed mechanism under rigorous security treatment. To demonstrate the generality of our mechanism and further enrich the application spectrum, we also show our new construction naturally supports fuzzy search, a previously studied notion aiming only to tolerate typos and representation inconsistencies in the user searching input. The extensive experiments on Amazon cloud platform with real data set further demonstrate the validity and practicality of the proposed mechanism.

DACMACS: Effective Data Access Control for Multiauthority Cloud Storage Systems

Data access control is an effective way to ensure data security in the cloud. However, due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Existing access control schemes are no longer applicable to cloud storage systems, because they either produce multiple encrypted copies of the same data or require a fully trusted cloud server. Ciphertext-policy attribute-based encryption (CP-ABE) is a promising technique for access control of encrypted data. However, due to the inefficiency of decryption and revocation, existing CP-ABE schemes cannot be directly applied to construct a data access control scheme for multi authority cloud storage systems, where users may hold attributes from multiple authorities. In this paper, we propose data access control for multiauthority cloud storage (DAC-MACS), an effective and secure data access control scheme with efficient decryption and revocation. Specifically, we construct a new multi authority CP-ABE scheme with efficient decryption, and also design an efficient attribute revocation method that can achieve both forward security and backward security. We further propose an extensive data access control scheme (EDAC-MACS), which is secure under weaker security assumptions.

II PROPOSED SYSTEM

We propose LDSS, a framework of lightweight data-sharing scheme in mobile cloud (see Fig. 1). It has the following six components.

(1) Data Owner (DO): DO uploads data to the mobile cloud and share it with friends. DO determines the access control policies.

(2) Data User (DU): DU retrieves data from the mobile cloud.

(3) Trust Authority (TA): TA is responsible for generating and distributing attribute keys.

(4) Encryption Service Provider (ESP): ESP provides data encryption operations for DO.

(5) Decryption Service Provider (DSP): DSP provides data decryption operations for DU.

(6) Cloud Service Provider (CSP): CSP stores the data for DO. It faithfully executes the operations requested by DO, while it may peek over data that DO has stored in the cloud.

IV METHODOLOGY

System Framework:

The development of cloud computing and the popularity of smart mobile devices, people are gradually getting accustomed to a new era of data sharing model in which the data is stored on the cloud and the mobile devices are used to store/retrieve the data from the cloud. In these applications, people (data owners) can upload their documents and other files to the cloud and share these data with other people (data users) they like to share. CSPs also provide data management functionality for data owners. Since personal data files are sensitive, data owners are allowed to choose whether to make their data files public or can only be shared with specific data users. Clearly, data privacy of the personal sensitive data is a big concern for many data owners. We propose LDSS, a framework of lightweight data sharing scheme in mobile cloud. It has the following six components. (1) Data Owner (DO) (2) Data User (DU) (3) Trust Authority (TA) (4) Encryption Service Provider (ESP) (5) Decryption Service Provider (DSP) (6) Cloud Service Provider (CSP).

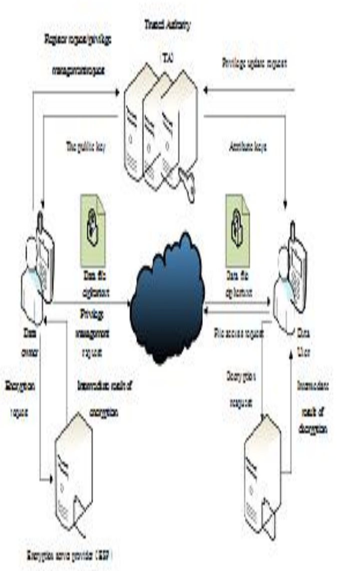

Fig: A lightweight data-sharing scheme (LDSS) framework.

Data Owner (DO):

When the data owner (DO) registers on TA, TA runs the algorithm Setup () to generate a public key PK and a master key MK. PK is sent to DO while MK is kept on TA itself. DO defines its own attribute set and assigns attributes to its contacts. All this information will be sent to TA and the cloud. TA and the cloud receive the information and store it. DO uploads data to the mobile cloud and share it with friends. DO determines the access control policies. DO sends data to the cloud. Since the cloud is not credible, data has to be encrypted before it is uploaded. The DO defines access control policy in the form of access control tree on data files to assign which attributes a DU should obtain if he wants to access a certain data file.

Data User (DU):

DU logins onto the system and sends, an authorization request to TA. The authorization request includes attribute keys (SK) which DU already has. TA accepts the authorization request and checks the request and a generate attribute keys (SK)for DU. DU sends a request for data to the cloud. Cloud receives the request and checks if the DU meets the access requirement. DU receives the ciphertext, which include ciphertext of data files and ciphertext of the symmetric key. DU decrypt the ciphertext of the symmetric key with the assistance of DSP. DU uses the symmetric key to decrypt the ciphertext of data files.

Trusted Authority:

To make LDSS feasible in practice, a trusted authority (TA) is introduced. It is responsible of generating public and private keys, and distributing attribute keys to users. With this mechanism, users can share and access data without being aware of the encryption and decryption operations. We assume TA is entirely credible, and a trusted channel exists between the TA and every user. The fact that a trusted channel exists doesn't mean that the data can be shared through the trusted channel, for the data can be in a large amount. TA is only used to transfer keys (in a small amount) securely between users. In addition, it's requested that TA is online all the time because data users may access data at any time and need TA to update attribute keys.

Cloud Service Provider:

CSP stores the data for DO. It faithfully executes the operations requested by DO, while it may peek over data that DO has stored in the cloud. DU sends a request for data to the cloud. Cloud receives the request and checks if the DU meets the access requirement. If DU can't meet the requirement, it refuses the request; otherwise it sends the ciphertext to DU. CSP manages the Uploaded Files.

V CONCLUSION

In recent years, many studies on access control in cloud are based on attribute-based encryption algorithm (ABE). However, traditional ABE is not suitable for mobile cloud because it is computationally intensive and mobile devices only have limited resources. In this paper, we propose LDSS to address this issue. It introduces a novel LDSS-CP-ABE algorithm to migrate major computation overhead from mobile devices onto proxy servers, thus it can solve the secure data sharing problem in mobile cloud. The experimental results show that LDSS can ensure data privacy in mobile cloud and reduce the overhead on users' side in mobile cloud. In the future work, we will design new approaches to ensure data integrity. To further tap the potential of mobile cloud, we will also study how to do ciphertext retrieval over existing data sharing schemes.

VI REFERENCES

[1] Gentry C, Halevi S. Implementing gentry's fully-homomorphic encryption scheme. in: Advances in Cryptology–EUROCRYPT 2011. Berlin, Heidelberg: Springer press, pp. 129-148, 2011.

[2] Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE. in: Proceeding of IEEE Symposium on Foundations of Computer Science. California, USA: IEEE press, pp. 97-106, Oct. 2011.

[3] Qihua Wang, Hongxia Jin. "Data leakage mitigation for discretionary access control in collaboration clouds". the 16th ACM Symposium on Access Control Models and Technologies (SACMAT), pp.103-122, Jun. 2011.

[4] Adam Skillen and Mohammad Mannan. On Implementing Deniable Storage Encryption for Mobile Devices. the 20th Annual Network and Distributed System Security Symposium (NDSS), Feb. 2013.

[5] Wang W, Li Z, Owens R, et al. Secure and efficient access to outsourced data. in: Proceedings of the 2009 ACM workshop on Cloud computing security. Chicago, USA: ACM pp. 55-66, 2009.

[6] Maheshwari U, Vingralek R, Shapiro W. How to build a trusted database system on untrusted storage. in: Proceedings of the 4th conference on Symposium on Operating System Design & Implementation-Volume 4. USENIX Association, pp. 10-12, 2000.

[7] Kan Yang, Xiaohua Jia, Kui Ren: Attribute-based fine-grained access control with efficient revocation in cloud storage systems. ASIACCS 2013, pp. 523-528, 2013.

[8] Crampton J, Martin K, Wild P. On key assignment for hierarchical access control. in: Computer Security Foundations Workshop. IEEE press, pp. 14-111, 2006.

[9] Shi E, Bethencourt J, Chan T H H, et al. Multi-dimensional range query over encrypted data. in: Proceedings of Symposium on Security and Privacy (SP), IEEE press, 2007. 350- 364

[10] Cong Wang, Kui Ren, Shucheng Yu, and Karthik Mahendra Raje Urs. Achieving Usable and Privacy-assured Similarity Search over Outsourced Cloud Data. IEEE INFOCOM 2012, Orlando, Florida, March 25-30, 2012

[11] Yu S., Wang C., Ren K., Lou W. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. INFOCOM 2010, pp. 534-542, 2010

[12] Kan Yang, Xiaohua Jia, Kui Ren, Bo Zhang, Ruitao Xie: DACMACS: Effective Data Access Control for Multiauthority Cloud Storage Systems. IEEE Transactions on Information Forensics and Security, Vol. 8, No. 11, pp.1790-1801, 2013.

[13] Stehlé D, Steinfeld R. Faster fully homomorphic encryption. in: Proceedings of 16th International Conference on the Theory and Application of Cryptology and Information Security. Singapore: Springer press, pp.377-394, 2010.

[14] 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.

[15] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption in: Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP). Washington, USA: IEEE Computer Society, pp. 321-334, 2007.

[16] Liang Xiaohui, Cao Zhenfu, Lin Huang, et al. Attribute based proxy re-encryption with delegating capabilities. in: Proceedings of the 4th International Symposium on Information, Computer and Communications Security. New York, NY, USA: ACM press, pp. 276-286, 2009.

[17] Pirretti M, Traynor P, McDaniel P, et al. Secure attribute-based systems. in: Proceedings of the 13th ACM Conference on Computer and Communications Security. New York, USA: ACM press, pp. 99-112, 2006.

[18] 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.

[19] Sandhu R S, Coyne E J, Feinstein H L, et al. Role-based access control models. Computer, 29(2): 38-47, 1996.

[20] Tian X X, Wang X L, Zhou A Y. DSP RE-Encryption: A flexible mechanism for access control enforcement management in DaaS. in: Proceedings of IEEE International Conference on Cloud Computing. IEEE press, pp.25-32, 2009

[21] Di Vimercati S D C, Foresti S, Jajodia S, et al. Over-encryption: management of access control evolution on outsourced data. in: Proceedings of the 33rd international conference on Very large data bases. Vienna, Austria: ACM, pp. 123-134, 2007.

[22] 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.

[23] 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.

[24] D. Huang, X. Zhang, M. Kang, and J. Luo. Mobicloud: A secure mobile cloud framework for pervasive mobile computing and

communication. in: Proceedings of 5th IEEE International Symposium on Service-Oriented System Engineering. Nanjing, China: IEEE, pp. 90-98, 2010.

[25] Benjamin Livshits, Jaeyeon Jung. Automatic Mediation of Privacy-Sensitive Resource Access in Smartphone Applications. USENIX Security, pp.113-130, Aug. 2013.

[26] Zhou Z, Huang D. Efficient and secure data storage operations for mobile cloud computing. in: Proceedings of 8th International Conference on Network and Service Management (CNSM 2012), Las Vegas, USA: IEEE, pp. 37-45, 2012.

[27] P. K. Tysowski and M. A.Hasan. Hybrid attribute- and reencryption-based key management for secure and scalable mobile applications in clouds. IEEE Transactions on Cloud Computing, vol. 1, no. 2, pp. 172-186, Nov. 2013.

[28] Boneh D, Franklin M. Identity-based encryption from the Weil pairing. in: Proceedings of the Advances in Cryptology. Berlin, Heidelberg: Springer-Verlag, pp. 213−229, 2001.

[29] Sahai A, Waters B. Fuzzy identity-based encryption. in: Proceedings of the Advances in Cryptology. Aarhus, Denmark: Springer-Verlag, pp.457-473, 2005.

[30] Shamir A. How to share a secret. Communications of the ACM,1979, 22 (11): 612-613.

SIVANI ARDHAMALA she is a master of Computer Science (M.Sc) pursuing in Sri Venkateswara University, Tirupati, A.P. She received Degree of Bachelor of Science in 2017 from Vikrama Simhapuri University, Nellore. Her research interests are Python, and Big Data.