A Novel Approach Of Data Sharing Scheme With Lightweight Secured For Cloud Computing

[1]KANAPARTHI NAGAMANI, [2] K.RAMA KRISHNA
[1]M.tech-Scholar, Dept of CSE, Chintalapudi Engineering College, Ponnur, A.P, India
[2]Assistant Professor, Dept of CSE, Chintalapudi Engineering College, Ponnur, A.P, India

ABSTRACT: *With the demand of cloud computing, mobile devices can store/retrieve personal data from anywhere at any time. Consequently, the data security problem in mobile cloud becomes more severe and prevents further development of mobile cloud. There are substantial studies that have been conducted for improving the cloud security. However, most of them are not applicable for mobile cloud since mobile devices only have limited computing resources and power. Solutions with low computational overhead are in great requirement for mobile cloud applications. In this paper, we propose a lightweight data sharing scheme (LDSS) for cloud computing of mobile. It adopts CP-ABE, an access control technology utilized in normal cloud environment, but changes the structure of access control tree to make it suitable for mobile cloud environments. LDSS moves a large portion of the computational intensive access control tree transformation in CP-ABE from mobile devices for external proxy servers. Furthermore, for reducing the user revocation cost, it introduces attribute description fields for implementing lazy-revocation, which is a thorny issue in program based CP-ABE systems. The experimental results exhibit that LDSS can effectively reduce the overhead on the mobile device side when users are sharing data in mobile cloud environments.*

Index Terms: mobile cloud computing, data encryption, access control, user revocation

I. INTRODUCTION

with 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 utilized to store/retrieve the data from the cloud.

Typically, mobile devices only have limited space of storage and computing power. On the contrary, the cloud has enormous amount of resources. In such a scenario, to achieve the satisfactory performance, it is essential to use the resources provided by the cloud service provider (CSP) to store and share the data. Nowadays, various cloud mobile applications have been widely used. In these applications, people (data owners) can upload their photos, videos, documents and other files to the cloud and share these data with other people (data users) they like to share. CSPs also give data management functionality for data owners. Since personal data files are sensitive, data owners are allowed to select 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 several data owners.

The state-of-the-art privilege management/access control mechanisms provided by the CSP are either not sufficient or not very convenient. They cannot meet all the requirements of data owners. First, when people upload their data files onto the cloud, they are leaving the data in a place where is out of their control, and the CSP may spy on user data for its commercial interests and/or other reasons. Second, people have to send password to each data user if they only want to share the encrypted data with certain users, which is very cumbersome. To simplify the privilege management, the data owner can divide data users into different groups and send password to the groups which they want to share the data. However, this approach requires fine-grained access control. In both cases, password management is a big issue.

Cloud computing means storing data and accessing that data from the Internet instead of utilizing Traditional hardware for most of the operations. More than 50% of companies in IT have moved their Business to the cloud. Sharing of data over the cloud is the modern trend that is being set on. The amount of 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. 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.

Therefore, privacy of the personal sensitive data is a big concern for many data owners. When any of the people upload the data onto the cloud they are leaving their data in a place 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 data should be encrypted before uploading it onto the cloud which can be safe from everyone.

Now the data encryption part brings some new problems such as we have to provide an efficient encryption algorithm such that if the data Is in encrypted format it cannot be easily to get break or get accessed by any exploiters. The next big concern is time consumption for encryption. Traditional Hardware with big configuration can encrypt data in short amount of time but limited resource devices suffer from this problem. They require more amount of time of encryption and decryption. So, an efficient crypto system is to be proposed which can worked equally or heterogeneously on all of the devices.

II. RELATED WORK

Attribute-based encryption (ABE) is proposed by Sahai and Waters. Attribute-based encryption (ABE) is a moderately late approach that re-evaluates the idea of public key cryptography. Attribute-based encryption is also referred to as ABE is a sort of public-key encryption wherein the secret key of a person and the cipher-text is established upon attributes. In an ABE, a

person's keys and cipher-texts are labeled with units of descriptive attributes and a symmetric key can decrypt a selected cipher-text only if there's a match between the attributes of the cipher-text and the person's key. It reduces the quantity of key utilized and hence makes encryption and decryption technique faster.

Secure and efficient access to outsourced data cloud providing secure and proficient admission to vast scale information is a critical segment figuring. In this rag, a PKI- based admittence control instrument is proposed. The component depends on encryption-based access control and over-encryption, it not just assurances secure admission to the outsourced data, but likewise soothe the data managers from client's each entrance technique, following stay away from the proprietor will turn into the bottleneck amid the entrance and archieve high pro- efficiency. Moreover, the component is simple and adaptable when clients are conceded or repudiated. Preparatory examination shows the adequacy and security of the system.

Cloud leagues are another joint effort worldview where associations share information over their remote cloud frameworks. In any case, the appropriation of cloud alliances is prevented by unified associations' worries on potential dangers of information spillage and information abuse. For cloud leagues to be practical, united associations' security concerns should to be lightened by giving instruments that enable associations to control which clients from other combined association's container get to which information We propose a novel personality and access administration framework for cloud alliances.

The framework enables united associations to uphold trait construct get to control arrangements in light of their data in a security saving style. Clients are allowed access to combined information when their character characteristics coordinate the strategies, however without uncovering their ascribes to the unified association owning data. The framework additionally ensures the honesty of the approach assessment process by utilizing piece chain innovation and Intel SGX put standard in equipment. It uses block chain to ensure that user's identity attributes and entree control policies cannot be modified by a malicious user, while Intel SGX protects the integrity what's more, privacy of the approach requirement process. We display the entrance control convention, the framework engineering and talk about future augmentations.

III. PROPOSED SYSTEM

ARCHITECTURE FLOW: Below architecture diagram represents mainly flow of request from the users to database through servers. In this scenario overall system is designed in three tiers separately utilizing three layers called presentation layer, business layer, data link layer. This project was developed by using 3-tier architecture.

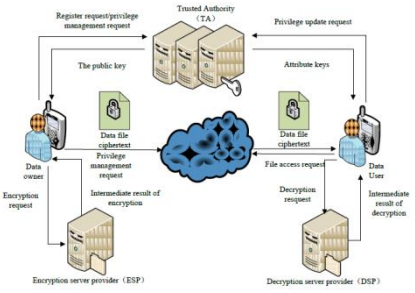

FIG 1: PROPOSED SYSTEM

The three-tier software architecture (a three layer architecture) emerged to overcome the limitations of the two-tier architecture. The third tier (middle tier server) is between the user interface (client) and the data management (server) components. This middle tier gives process management where business logic and rules are executed and can accommodate hundreds of users (as compared to only 100 users with the two tier architecture) by providing functions like queuing, application execution, and database staging.

The three tier architecture is utilized when an effective distributed client/server design is needed that provides (when compared to the two tier) maximized performance, flexibility, maintainability, reusability, and scalability, while hiding the complexity of distributed processing from the user. These characteristics have made three layer architectures a popular choice for Internet applications and net-centric information systems.

In our proposed system data is encrypted before uploading to the cloud. Combination of Attribute Based Encryption and Byte Rotation Algorithm are utilized for the encryption of the data. ABE will help to identify the attributes of the data and BREA will perform matrix operations on the block of the data to be encrypted. After performing encryption operation, a random key is generated alongside the encrypted data. Data will be sent in encrypted format to respective user. To decrypt this data receiver has to enter the One Time Password (OTP) which will be matched with key generated using ABE algorithm.

IV. RESULTS

FIG 2: HOME PAGE

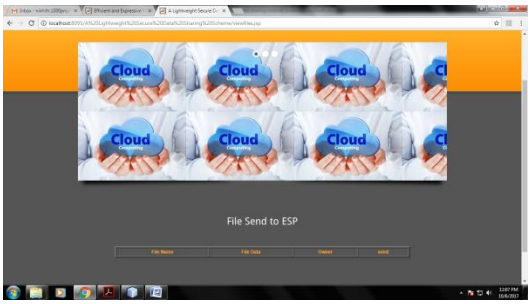

FIG 3: FILE SEND TO ESP

FIG 4: FILE UPLOAD TO CLOUD

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 cipher text retrieval over existing data sharing schemes.

VI. REFENRENCES

[1] P. K. Tysowski and M. A.Hasan. Hybrid attribute- and re-encryption-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.

[2] 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.

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

[4] 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.

[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, XiaohuaJia, KuiRen: 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 hierarchicalaccess 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, KuiRen, Shucheng Yu, and KarthikMahendraRajeUrs. 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, XiaohuaJia, KuiRen, Bo Zhang, RuitaoXie: DAC-MACS: 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 key-policy 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.

KANAPARTHI NAGAMANI completed her B.TECH at D.M.S.S.V.H College of Engineering, MachiliPatnam. She is pursuing her M.TECH in Chintalapudi Engineering College, Ponnur. Her Specialization is Computer Science Engineering (CSE).

K.RAMA KRISHNA completed his B.TECH in Narasaraopeta Engineering College and M.TECH in School of Information Technology (JNTUH). He is working as Assistant Professor in Chintalapudi Engineering College, Ponnur. He has 11Years of EXPERIENCE. His area of interest is Data warehousing and Mining.