International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN: 2456-172X | Vol. 2, No. 1, March - May, 2017 | Pages 105-110

P-MOD: SECURE PRIVILEGE-BASED MULTILEVEL ORGANIZATIONAL DATA-SHARING IN CLOUD COMPUTING

G.KEERTHANA[1], K.PUSHPAVALLI[2]

Department of Information Technology, Agni College Of Technology, Chennai.

Abstract- In the Proposed System, a privilege- based access structure can facilitate organizations in applying big data analytics to understand populations in a holistic way. A Privilege-based Multilevel Organizational Data-sharing scheme (P- MOD) that incorporates a privilege-based access structure into an attribute-based encryption mechanism to handle the management and sharing of big data sets. It builds on concepts presented in to solve the problems of sharing data within organizations with complex hierarchies. It helps to reduce the complexity of defining hierarchies as the number of users grows. The comprehensive performance and simulation analyses using the real Census Income data set demonstrate that P-MOD is more efficient.

1. INTRODUCTION

The title of the project is "P-MOD: Secure Privilege-Based Multilevel Organizational Data-Sharing in Cloud Computing". Cloud computing has changed the way enterprises store, access and share data. Big data sets are constantly being uploaded to the cloud and shared within a hierarchy of many different individuals with different access privileges. With more data storage needs turning over to the cloud, finding a secure and efficient data access structure has become a major research issue. Here a Privilege-based Multilevel Organizational Data-sharing scheme (P-MOD) is proposed that incorporates a privilege-based access structure into an attribute-based encryption mechanism to handle the management and sharing of big data sets. This system, privilege-based access structure helps reduce the complexity of defining hierarchies as the number of users grow.

2.Related Work

Most attribute based encryption schemes such as Fuzzy IBE, KP-ABE, and CP-ABE serve as a better solution when data users are not ranked into a hierarchy and each is independent of one another. However, they share a common limitation of high computational complexity in the case of large multilevel organizations. These schemes require a single data file to be encrypted with a large number of attributes (from different levels) to grant them access to it.

- **Identity-Base Encryption (Fuzzy IBE) was introduced in to handle data sharing on the cloud in a flexible approach using encryption.**The cipher-text is shared on the cloud to restrict access to authorized users. In order for an authorized individual to obtain the data, the user must request a private key from a key-issuer to decrypt the encrypted data.
- **Attribute-Based Encryption (ABE) schemes later emerged to provide more versatility when sharing data.**These schemes integrate two types of constructs: attributes and access policies. Access policies are statements that join attributes to express which users of the

system are granted access and which users are denied. ABE schemes were introduced via two different approaches: Key-Policy Attribute-Based Encryption (KPABE) and Cipher-text Policy Attribute-Based Encryption (CP-ABE). In KP-ABE, each cipher-text is labeled with a set of descriptive attributes, while each private key is integrated with an access policy. For authorized data users to decrypt the cipher-text, they must first obtain a private key from the key-issuer to use in decryption. The key-issuer integrates the access policy into the keys generated. Data users can successfully decrypt a cipher-text if the set of descriptive attributes associated with the cipher-text satisfies the access policy integrated within their private keys.

- CP-ABE is considered to be conceptually similar to Role-Based Access Control (RBAC). It gives the data owner control over which data user is able to decrypt certain cipher-texts. This is due to the access structure being integrated by the data owner into the cipher-text during encryption. It allows the private key generated by the key-issuer to only contain the set of attributes possessed by the data user. Some CP-ABE schemes were later introduced that can provide higher flexibility and better efficiency.

To mitigate financial loss and implications on the reputation associated with data breaches, large multilevel organizations, such as healthcare networks, government agencies, banking institutions, commercial enterprises and etc., began allocating resources into data security research to develop and improve accessibility and storage of highly sensitive data.

3. PROPOSED SYSTEM

Our proposed system is privilege-based access structure. It can also facilitate organizations in applying big data analytics to understand populations in a holistic way. A Privilege-based Multilevel Organizational Data-sharing scheme (P-MOD) is proposed. It builds on concepts presented in to solve the problems of sharing data within organizations with complex hierarchies. Multiple data file partitioning techniques and propose a privilege-based access structure that facilitate data sharing in hierarchical settings. We formally prove the security of P-MOD and show that it is secure against adaptively chosen plaintext attacks under the Decisional Bilinear Diffie-Hellman (DBDH) assumption. Present a performance analysis for P-MOD and compare it to three existing schemes that aim to achieve similar hierarchical goals. We implement P-MOD and conduct comprehensive simulations under various scenarios using the real Census Income data set.

3.1 Techniques

The advantages of our proposed privilege-based access structure is the ability to reduce attribute replication when defining the hierarchy. Based on the composition of our proposed access structure which does not duplicate attributes, therefore generates smaller cipher-texts. A formal proof of security for P-MOD is presented. It is assumed that a symmetric encryption technique such as AES is used to secure each individual data file.CP-ABE(Cipher-Text Policy Atribute-Based Encryption) algorithm handles sharing of independent pieces of data based on independent access policies. It was not designed to support a privilege-based access structure.

3.2 Present Application

Hierarchical Attribute-Based Encryption (HABE) that combines the Hierarchical Identity-Based Encryption (HIBE) scheme and CP-ABE was later introduced. HABE is able to achieve fine-grained access control in a hierarchical organization. Its consists of a root master that generates and distributes parameters and keys, multiple domain masters that delegate keys to domain masters at the following levels, and numerous users. In this scheme, keys are generated in the same hierarchical key generation approach as the HIBE scheme.

3.3 Algorithm

FH-CP-ABE

File Hierarchy Cipher-text Policy Attribute-Based Encryption (FH-CP-ABE) is one of the most recent hierarchical solutions available today. It proposes a leveled access structure to manage a hierarchical organization that shares data of various sensitivity. A single access structure was proposed that represents both the hierarchy and the access policies of an organization. This access structure consists of a root node, transport nodes, and leaf nodes. The root node and transport nodes are in the form of gates (i.e. AND or OR). The leaf nodes represent attributes that are possessed by data users.

Parameters

Based on the possession of certain attributes, each data user is mapped into specific transport nodes (certain levels within the hierarchy) based on the access structure that the user satisfies. If the data user satisfies a full branch of the access structure, then the data user is ranked at the root node (highest level within the hierarchy). Data users ranked at the highest level (root node) can decrypt a cipher-text of highest sensitivity and any other cipher-text with less sensitivity in the lower levels of the hierarchy. The nodes ranked in the lower levels (transport nodes) can not decrypt any ciphertexts in the levels above. The main advantage of this scheme is that it provides leveled access structures which are integrated into a single access structure.However, in real-life applications, relationships within an organization are often built in a cross-functional matrix, making this a complicated solution when assigning privileges.

Cryptographic Hash Function

A cryptographic hash function h is a mathematical algorithm that maps data of arbitrary size to a bit string of fixed size.

Bilinear Maps

Multiplicative cyclic groups of the same prime order. Decisional Bilinear Diffie-Hellman (DBDH) Assumption. The DBDH assumption is a computational hardness assumption.

Access Structure

An access structure represents access policies for a set of individuals interested in gaining individual access to a secret. The access structure defines sets of attributes that can be possessed by a single individual to allow access to the secret.

Leveled Access Tree

An access tree level represents an access structure that determines whether a data user can decrypt the cipher-text.

3.4 Practical Implementation

Consider a data owner that possesses a data file and wishes to selectively share different segments of it on the cloud among a set of data users based on certain access privileges. We assume that the data users can be ranked into a hierarchy that defines their access privileges. Selectively sharing data files on the cloud becomes a burden on the data owner as the hierarchy grows (the access privileges increase in number) and/or as the access restrictions become more complex due to an increase in the sensitivity of the file segments. A trivial solution involves the data owner to use public key encryption. This solution would require the data owner to encrypt the same part of the data file once for each data user being granted access then upload the resulting cipher-texts to the cloud. The data users would then fetch their uniquely encrypted parts of the file from the cloud and utilize their private keys to decrypt them. This method ensures that

noun privileged data user will gain access to any part of the data file even if that user is able to download the cipher-texts from the cloud.

3.5 Advantages

1. Which makes managing healthcare records using mobile healthcare devices feasible.
2. Our system helps reduce the complexity of defining hierarchies as the number of users grows
3. The comprehensive performance and simulation analyses using the real Census Income data set demonstrate that P-MOD is more efficient
4. In computational complexity and storage space than the existing schemes.

4. MODULE DESCRIPTION

With the development of cloud storage, more data owners are inclined to outsource their data to cloud services. For privacy concerns, sensitive data should be encrypted before outsourcing. So the scope of our project is data security and privacy for multi owners. A tree-based index structure and an efficient search algorithm. The cloud server will merge encrypted indexes without knowing the corresponding sensitive information. The authenticated data user only needs to encrypt query keywords once to efficiently retrieve all files of interestBenefits Sharing.

4.1 Multiple Data Owner

With the character of low maintenance, cloud computing provides an economical and efficient solution for sharing group resource among cloud users. Unfortunately, sharing data in a multi-owner manner while preserving data and identity privacy from an un-trusted cloud is still a challenging issue, due to the frequent change of the membership. Secure multi-owner data sharing scheme for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users.

4.2Efficient Attribute-Based Encryption Scheme in Cloud Computing

Cipher-text-policy attribute-based encryption (CP-ABE) has been a preferred encryption technology to solve the challenging problem of secure data sharing in cloud computing. The shared data files generally have the characteristic of multilevel hierarchy, particularly in the area of healthcare and the military. However, the hierarchy structure of shared files has not been explored in CP-ABE. An efficient file hierarchy attribute-based encryption scheme is proposed in cloud computing. The layered access structures are integrated into a single access structure, and then, the hierarchical files are encrypted with the integrated access structure. The cipher-text components related to attributes could be shared by the files. Therefore, both cipher-text storage and time cost of encryption are saved.

4.3 Cloud Service Provide

The one who manages the cloud servers and provides multiple services for client is the Cloud Service Provider (CSP). A data owner can encrypt the data files and upload the generated cipher-text to CSP. A user can downloads and decrypts the cipher-text from CSP. These shared files must have hierarchical structure. That is many hierarchy subgroups or a group of files may

be located at different access levels. If the files in the same hierarchical structure can be encrypted by using integrated access structure, then the storage cost of cipher-text and time cost of encryption could be saved. The hierarchical files are encrypted with an integrated access structure and the cipher-text components related to attributes could be shared by the files. The main advantage of this method is that users can decrypt all authorization files by computing secret key once.

4.4 Data User – From cloud

The cloud consumer is the principal stakeholder for the cloud computing service. A cloud consumer represents a person or organization that maintains a business relationship with, and uses the service from a cloud provider. A cloud consumer browses the service catalog from a cloud provider, requests the appropriate service, sets up service contracts with the cloud provider, and uses the service. The cloud consumer may be billed for the service provisioned, and needs to arrange payments accordingly. Cloud consumers need SLAs to specify the technical performance requirements fulfilled by a cloud provider. SLAs can cover terms regarding the quality of service, security, remedies for performance failures. A cloud provider may also list in the SLAs a set of promises explicitly not made to consumers, i.e. limitations, and obligations that cloud consumers must accept. A cloud consumer can freely choose a cloud provider with better pricing and more favourable terms.

5. SCOPE FOR DEVELOPMENT OF THIS PROJECT

More data storage needs turning over to the cloud,

- Finding a secure and efficient data access structure.
- Store, access and share data.
- Being uploaded to the cloud and shared within a hierarchy of many different individuals with different access privileges.

6.CONCLUSION

This paper begins by pointing out major security concerns data owners have when sharing their data on the cloud. Next, the most widely implemented and researched data sharing schemes are briefly discussed revealing points of weakness in each. To address the concerns, this paper proposes a Privilege-based Multilevel Organizational Datasharing scheme (P-MOD) that allows data to be shared efficiently and securely on the cloud. P-MOD partitions a data file into multiple segments based on user privileges and data sensitivity. Each segment of the data file is then shared depending on data user privileges. We formally prove that P-MOD is secure against adaptively chosen plaintext attack assuming that the DBDH assumption holds. Our comprehensive performance and simulation comparisons with the three most representative schemes show that P-MOD can significantly reduce the computational complexity while minimizing the storage space. Our proposed scheme lays a foundation for future attribute-based, secure data management and smart contract development.

REFERENCES

a) P. Institute, "Sixth annual benchmark study on privacy and security of healthcare data," tech. rep., Ponemon Institute LLC, 2016.

b) R. Cohen, "The cloud hits the mainstream: More than half of U.S. businesses now use

cloud computing." http://www.forbes.com, April 2013. Online; posted 10-January-2017.
c) E. Zaghloul, T. Li, and J. Ren, "An attribute-based distributed data sharing scheme," in IEEE Globeocm 2019, (Abu Dhabi, UAE.), 9-13 December 2018.
d) Yoshiko Yasumura, Hiroki Imabayashi, " Attribute-based Proxy Re-encryption Method for Revocation in Cloud Storage: Reduction of Communication Cost at Re-encryption" 2018.
e) NSandeep Chaitanya1,S Ramachandram2," Usage of DHS and De-duplicating Encrypted Data using ABE & ECC for Secured Cloud Environment" 2018.
f) Quist-Aphetsi, Kester1,2,3, Blankson, Henry2,4 "A Hybrid Data Logging System Using Cryptographic Hash Blocks Based on SHA-256 and MD5 for Water Treatment Plant and Distribution Line" 2019.
g) Xiaotong Sun, "Critical Security Issues in Cloud Computing: ASurvey" September 04,2020.
h) Fekadu workneh, Ahmed Adem, Ms.Roshni Pradhan, "Understanding Cloud Based Health Care Service with Its Benefits" 2018.
i) Adavi Madhavi, Susan Lincke, "SecurityRisk Assessment in Electronic Health Record System " 2018.
j) Harsh Gupta, Deepak Kumar, "Security Threats in Cloud Computing" 2019.
k) Abdelali El Bouchti, Samir Bahsani, Tarik Nahhal, "Encryption as a Service for Data Healthcare Cloud Security" 2016.
l) S.Petcy Carolin, M.Somasundaram, "DATA LOSS PROTECTION AND DATA SECURITY USING AGENTS FOR CLOUD ENVIRONMENT" 2016.
m) Shariqua Izhar, Anchal Kaushal, Ramsha Fatima, Mohammed A. Qadeer, "Enhancement in Data Security using Cryptography and Compression " 2017.
n) Dr. S.Pariselvam, M.Swarnamukhi, "Encrypted Cloud Based Personal Health Record Management Using DES Scheme" 2019.

o) DIAO Zhe, WANG Qinghong, SU Naizheng, ZHANG Yuhan, "Study on Data Security Policy Based On Cloud Storage" 2017.

p) Sangeetha.M, Dr.P.VijayaKarthik, "To provide a secured access control using combined hybrid Key-Ciphertext Attribute based encryption (KC-ABE) " 2017.

q) Dheeraj Selar G, Apoorva P, "Comparative Study on KP-ABE and CP-ABE Algorithm for Secure Data Retrieval in Military Network" 2017.

r) G. Wang, Q. Liu, J. Wu, and M. Guo, "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers," Computers & Security, vol. 30, no. 5, pp. 320–331, 2011.

s) P. Mell and T. Grance, "The NIST definition of cloud computing," 2011.

t) S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen, and W. Xie, "An efficient file hierarchy attribute-based encryption scheme in cloud computing," IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1265–1277, 2016.