P-MOD: Secure Privilege-Based Multilevel Organizational Data- Sharing in Cloud Computing

Keerthana G[1], Kalaiselvi V[2], Nivi V[3]
[1]*Assistant Professor, Dept. of Information Technology, Agni College of Technology, Chennai*
[2,3]*UG Student, Dept. 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. To handle the management and sharing of the large data sets, a Privilege-based Multilevel Organizational Data-sharing (P-MOD) scheme is proposed which incorporates a privilege-based access structure into an attribute-based encryption mechanism. 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.**

Index Terms **- Cloud Computing, Hierarchy, Privilege-based Access, attribute-based encryption, CP-ABE, MD5.**

I.INTRODUCTION

Our title of the project is "P-MOD: Secure Privilege-Based Multilevel Organizational Data-Sharing in Cloud Computing". The way enterprises store, access and share data has been changed using cloud computing. In Cloud Computing, the large data sets are uploaded and shared within a hierarchy of many different individuals with different with different access privileges. If more data storage occurs it turns over to the cloud. The major research issue is finding a secure and efficient data access structure. To handle the management and sharing of the large data sets, a Privilege-based Multilevel Organizational Data-sharing (P-MOD) scheme is proposed which incorporates a privilege-based access structure into an attribute-based encryption mechanism. This system, privilege-based access structure helps reduce the complexity of defining hierarchies as the number of users grow.

II. RELATED WORK

The Fuzzy Identity Based Encryption (IBE), Cipher Policy – Attribute Based Encryption (CP-ABE) and Key Policy – Attribute Based Encryption (KP-ABE) are the most attribute-based encryption that serve as a better solution when data users are not ranked into hierarchy and each is independent of one another. In the case of large multilevel organizations, they share a common limitation of high computational complex. The requirement to grant them access to these schemes is a single data file to be encrypted with a large number of attributes (from different levels).

- 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 person 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. To express the users system grant access and users system denial it joins attributes called access policies (which is a statement). 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 keys generated in the access policy are integrated by key-issuer. 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 should 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 the encryption process. The key-issuer generate a private key that allows to 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 to develop and improve accessibility and storage of highly sensitive data we allocate resources into data security research.

III. PROPOSED SYSTEM

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

A. 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. The security of P-MOD is presented in this. It is assumed that a symmetric encryption technique such as AES is used to secure each individual data file. CP-ABE (Cipher-Text Policy Attribute-Based Encryption) algorithm handles sharing of independent pieces of data based on independent access policies. A privilege-based access structure that it was not designed to support.

B. Present Application

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

C. Algorithm

FH-CP-ABE

File Hierarchy Cipher-text Policy Attribute-Based Encryption (FH-CP-ABE) is one of the most recent hierarchical solutions that are available today. A hierarchical organization manages by sharing the data of various sensitivity by proposing a levelled access structure. A single access structure was proposed which represents both the hierarchy and the access policies of an organization. A single access structure consists of a root node, transport nodes, and leaf nodes. The root node and transport nodes are in the form of gates such as AND gate or OR gate. The leaf nodes represent the attributes that are possessed by the data users.

1.Parameter

Based on the access structure that the user satisfies, each data user is mapped into specific transport nodes (certain levels within the hierarchy). If the data user that satisfies a full branch of the access structure, then the data user is ranked at the root node (highest level within hierarchy). A cipher-text of highest sensitivity can decrypt by high level (root node) data users,). A cipher-text of lowest sensitivity can decrypt by low level data users. The nodes ranked in the lower levels (i.e.: transport nodes) cannot decrypt any ciphertexts in the above levels. The advantage of P-MOD scheme is that it facilitates leveled access structures which are

integrated into a single access structure. The application of real-life time, relationships within an organization are often built-in a cross-functional matrix, making this a complicated solution when assigning privileges.

2.Cryptographic Hash Function

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

3.Bilinear Maps

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

4.Access Structure

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

5.Leveled Access Tree

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

D. Advantages

- Which makes managing healthcare records using mobile healthcare devices feasible.
- Our system helps 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
- In computational complexity and storage space than the existing schemes.

E. System Design

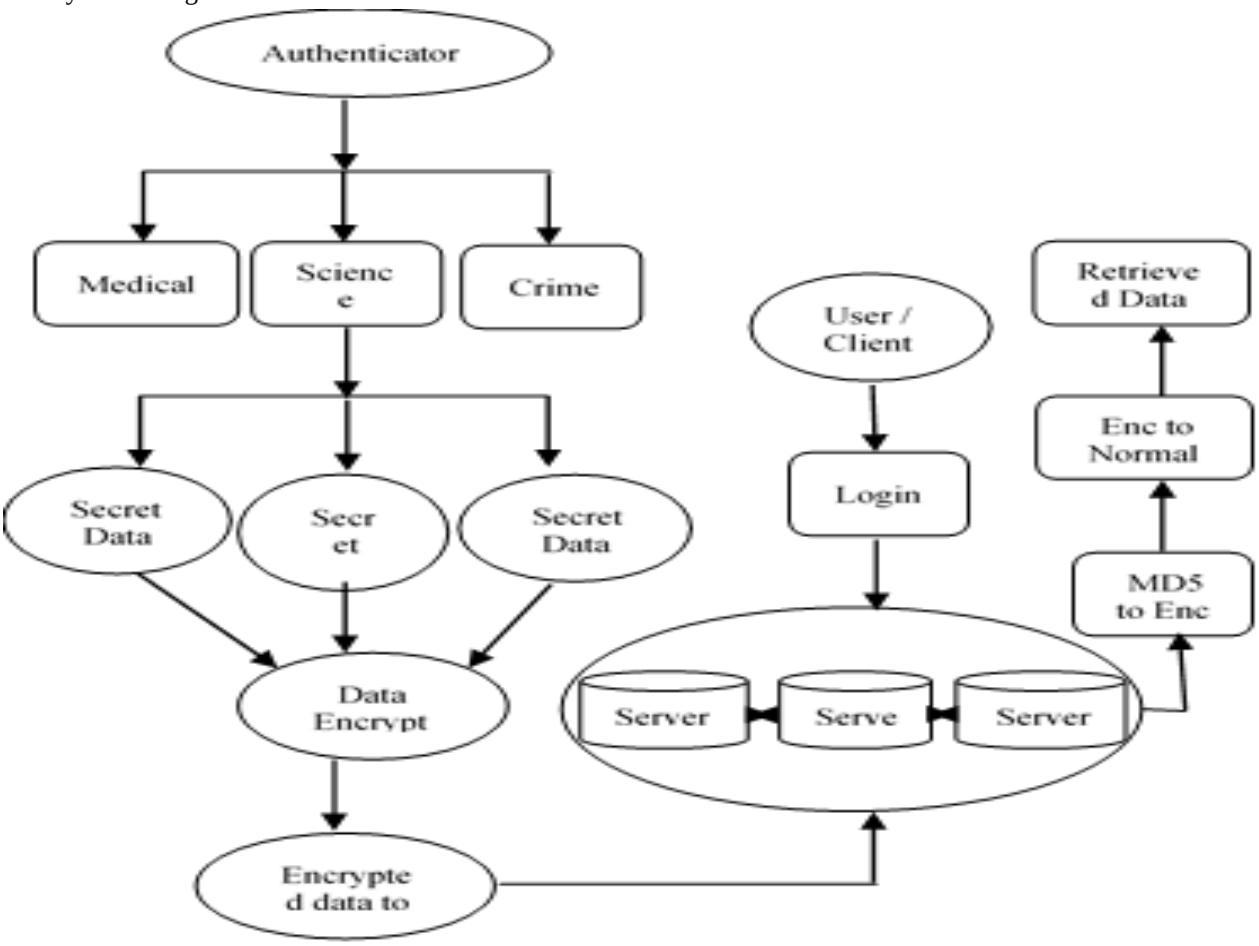

Fig. 3.1 Systems Architecture

IV. MODULE DESCRIPTION

To outsource their data to cloud services the more data owners are inclined with the development of cloud storage, before outsourcing due privacy concerns, sensitive data should be encrypted. So, the aim of our project is data security and privacy for multi owners. Without knowing the corresponding sensitive information, the cloud server will merge encrypted indexes. The authenticated data user only needs to encrypt query keywords once to efficiently retrieve all files of interest benefits Sharing.

A. Multiple Data Owner

For sharing group resource among cloud users the main characteristics such as low maintenance, cloud computing provides an economical and efficient solution. Due to the frequent change of the membership the preserving data and identity privacy from an un-trusted cloud, sharing data in a multi-owner manner is still a challenging issue. The Secure multi-owner data sharing scheme for the dynamic groups in the cloud. Any cloud user can anonymously share data with others by leveraging group signature and dynamic broadcast encryption techniques. The storage will be overhead, and the encryption computation cost of our scheme are independent with the number of revoked users.

B. Efficient Attribute-Based Encryption Scheme in Cloud Computing

To solve the challenging problem of secure data sharing in the cloud computing the most preferred encryption technology is Cipher-text-policy attribute-based encryption (CP-ABE). The characteristic of multilevel hierarchy has the shared data files, particularly in the area of healthcare and the military. The shared file's the hierarchy structure is not explored in CP-ABE. In the cloud computing, an efficient file hierarchy attribute-based encryption scheme is proposed. A single access structure is an integration of the layered access structures. An Access structure is an integration of the hierarchical files that are encrypted. The cipher-text components related to attributes are shared in the form of files. Therefore, both the cipher-text storage and the time cost of encryption are saved.

C. Cloud Service Provider

The Cloud Service Provider (CSP) is the one who manages the cloud servers and provides multiple services for client. A data owner can encrypt the data files and upload the generated cipher-text to CSP. In CSP, a user can download and decrypts the cipher-text. These shared files must have hierarchical structure. A group of files that is many hierarchy subgroups is 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 encryption of hierarchical files with an integrated access structure and the cipher-text components related to the attributes that could be shared in the form of the files. The decryption of authorization files of users by computing secret key once is the main advantages of this method.

D. Data User – From cloud

The principal stakeholder for the cloud computing service is the cloud consumer. The cloud consumer (i.e.: a person or an organization) that represents who maintains a business relationship and uses the service from a cloud provider. For the service provisioned the cloud consumer may be billed and needs to arrange payments accordingly. To specify the technical performance requirements the cloud consumers, need SLAs fulfilled by a cloud provider. The terms regarding the quality of service, security, remedies for performance failures are covered by the SLAs. To consumers a set of promises explicitly are not made, i.e., limitations, and obligations may also list in the SLAs by a cloud provider that cloud consumers must accept. A freedom of choosing a cloud provider is given by cloud with better pricing and more favor-able terms.

V. CONCLUSION

When sharing the data on the cloud the major point to be concerned is data security of the owners which is highlighted in this paper. The most widely implemented and researched data sharing schemes are briefly discussed and revealing points of weakness in each. This paper proposes a Privilege-based Multilevel Organizational Data-sharing (P-MOD) scheme that allows data to be shared efficiently and securely on the cloud. Based on user privileges and data sensitivity, P-MOD partitions a data file into multiple segments. The sharing of each segment of the data file is depends on

data user privileges. In this we formally proved that the P-MOD is secure against the 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

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

[2] 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.

[3] 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.

[4] Yoshiko Yasumura, Hiroki Imabayashi, " Attribute-based Proxy Re-encryption Method for Revocation in Cloud Storage: Reduction of Communication Cost at Re-encryption" 2018.

[5] NSandeep Chaitanya1, S Ramachandram2," Usage of DHS and De-duplicating Encrypted Data using ABE & ECC for Secured Cloud Environment" 2018.

[6] 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.

[7] Xiaotong Sun, "Critical Security Issues in Cloud Computing: ASurvey" September 04,2020.

[8] Fekadu workneh, Ahmed Adem, Ms.Roshni Pradhan, "Understanding Cloud Based Health Care Service with Its Benefits" 2018.

[9] Adavi Madhavi, Susan Lincke, "Security Risk Assessment in Electronic Health Record System "2018.

[10] Harsh Gupta, Deepak Kumar, "Security Threats in Cloud Computing" 2019.

[11] Abdelali El Bouchti, Samir Bahsani, Tarik Nahhal, "Encryption as a Service for Data Healthcare Cloud Security" 2016.

[12] S.Petcy Carolin, M.Somasundaram, "DATA LOSS PROTECTION AND DATA SECURITY USING AGENTS FOR CLOUD ENVIRONMENT" 2016.

[13] Shariqua Izhar, Anchal Kaushal, Ramsha Fatima, Mohammed A. Qadeer, "Enhancement in Data Security using Cryptography and Compression "2017.

[14] Dr. S.Pariselvam, M.Swarnamukhi, "Encrypted Cloud Based Personal Health Record Management Using DES Scheme" 2019.

[15] DIAO Zhe, WANG Qinghong, SU Naizheng, ZHANG Yuhan, "Study on Data Security Policy Based on Cloud Storage" 2017.

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

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

[18] 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.

[19] P. Mell and T. Grance, "The NIST definition of cloud computing," 2011.

[20] 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.