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

[1]subiya khanam, [2]Dr.E.srikanth reddy
[1]M.Tech, CSE, Department of Computer Science, VAAGESWARI COLLEGE OF ENGINEERING Thimmapur, Karimnagar, Telangana, INDIA, H.No:20S41D5819, subiyakhanam18@gmail.com
[2]Professor, Department of Computer Science, VAAGESWARI COLLEGE OF ENGINEERING Thimmapur, Karimnagar, Telangana, INDIA, srikanth574@gmail.com

ABSTRACT: 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. In this paper, a Privilege-based Multilevel Organizational Data-sharing scheme (P-MOD) is proposed that incorporates a privilege-based access structure into an attributebased encryption mechanism to handle the management and sharing of big data sets. Our proposed privilege-based access structure helps reduce the complexity of defining hierarchies as the number of users grows, which makes managing healthcare records using mobile healthcare devices feasible. It can also facilitate organizations in applying big data analytics to understand populations in a holistic way. Security analysis shows that P-MOD is secure against adaptively chosen plaintext attack assuming the DBDH assumption holds. The comprehensive performance and simulation analyses using the real U.S. Census Income data set demonstrate that P-MOD is more efficient in computational complexity and storage space than the existing schemes.

Keywords *– Cloud computing, big data, hierarchy, privilege-based access, sensitive data, attribute-based encryption, mobile healthcare.*

1. INTRODUCTION

IT was estimated that data breaches cost the United States' healthcare industry approximately $6.2 billion in 2016 alone [1]. 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. One major way that large enterprises are adapting to increased sensitive data management is the utilization of the cloud environment. It was reported that more than half of all U.S. businesses have turned over to the cloud for their business data management needs [2]. The on-demand cloud access and data sharing can greatly reduce data management cost, storage flexibility, and capacity [3]. However, data owners have deep concerns when sharing data on the cloud due to security issues. Once uploaded and shared, the data owner inevitably loses control over the data, opening the door to unauthorized data access. A critical issue for data owners is how to efficiently and securely grant privilege level-based access rights to a set of data. Data owners are becoming more interested in selectively sharing information with data users based on different levels of granted privileges. The desire to grant level-based access results in higher computational complexity and complicates the methods in which data is shared on the cloud. Research in this field focuses on finding enhanced schemes that can securely, efficiently and intelligently share data on the cloud among users according to granted access levels.

2. LITERATURE REVIEW

Ciphertext-policy attributebased encryption

In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper we present a system for realizing complex access control on encrypted data that we call ciphertext-policy attribute-based encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous attribute-based encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods such as role-based access control (RBAC). In addition, we provide an implementation of our system and give performance measurements.

An efficient file hierarchy attribute-based encryption scheme in cloud computing

Ciphertext-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. In this paper, 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 ciphertext components related to attributes could be shared by the files. Therefore, both ciphertext storage and time cost of encryption are saved. Moreover, the proposed scheme is proved to be secure under the standard assumption. Experimental simulation shows that the proposed scheme is highly efficient in terms of encryption and decryption. With the number of the files increasing, the advantages of our scheme become more and more conspicuous.

CP-ABE with constant-size keys for lightweight devices

Lightweight devices, such as radio frequency identification tags, have a limited storage capacity, which has become a bottleneck for many applications, especially for security applications. Ciphertext-policy attribute-based encryption (CP-ABE) is a promising cryptographic tool, where the encryptor can decide the access structure that will be used to protect the sensitive data. However, current CP-ABE schemes suffer from the issue of having long decryption keys, in which the size is linear to and dependent on the number of attributes. This drawback prevents the use of lightweight devices in practice as a storage of the decryption keys of the CP-ABE for users. In this paper, we provide an affirmative answer to the above long-standing issue, which will make the CP-ABE very practical. We propose a novel CP-ABE scheme with constant-size decryption keys independent of the number of attributes. We found that the size can be as small as 672 bits. In comparison with other schemes in the literature, the proposed scheme is the only CP-ABE with expressive access structures, which is suitable for CP-ABE key storage in lightweight devices.

JPBC: Java pairing based cryptography AUTHORS: A. De Caro and V. Iovino

It has been recently discovered that some cyclic groups that could be used in Cryptography admit a special bilinear pairing map that introduces extra structure to the group. Bilinear pairing maps were first used to break cryptosystems (see, for example,) and later it was realized that the extra structure could be exploited to build cryptosystems with extra properties. Boneh and Franklins identity-based encryption scheme is the most famous early example of what could be achieved using bilinear maps. After that, a plethora of cryptosystems have been designed using bilinear maps. No full and freely available implementation of pairing based cryptography was available until this work. Recent proposals fall short of this goal as either their source code is not available or because they support a limited range of elliptic curve. Moreover, neither one of implements preprocessing that is crucial to reduce the computation time. In this work, we present jPBC a Java port of the PBC library written in C. jPBC provides a full ecosystem of interfaces and classes to simplify the use of the bilinear maps even for a non-cryptographer. jPBC supports different types of elliptic curves, preprocessing which can speed up the computation significantly and it is ready for the mobile world. Moreover, a benchmark comparison between jPBC and PBC has been performed to measure the gap between the two libraries. Furthermore, jPBC has been benchmarked on different Android mobile platforms.

Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers
With rapid development of cloud computing, more and more enterprises will outsource their sensitive data for sharing in a cloud. To keep the shared data confidential against untrusted cloud service providers (CSPs), a natural way is to store only the encrypted data in a cloud. The key problems of this approach include establishing access control for the encrypted data, and revoking the access rights from users when they are no longer authorized to access the encrypted data. This paper aims to solve both problems. First, we propose a hierarchical attribute-based encryption scheme (HABE) by combining a hierarchical identity-based encryption (HIBE) system and a ciphertext-policy attribute-based encryption (CP-ABE) system, so as to provide not only fine-grained access control, but also full delegation and high performance. Then, we propose a scalable revocation scheme by applying proxy re-encryption (PRE) and lazy re-encryption (LRE) to the HABE scheme, so as to efficiently revoke access rights from users.

3. METHODOLOGY

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 (i.e. no relationships).

- HABE is able to achieve fine-grained access control in a hierarchical organization. It 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. To express an access policy, HABE uses a disjunctive normal form where all attributes are administered from the same domain authority into one conjunctive clause

Disadvantages:

- 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.
- Synchronizing attribute administration might become a challenging issue with complex organizations that have multiple domain authorities ince this scheme uses a single access structure to represent the full hierarchy, the higher levels are forced to accommodate attributes of all the levels below. As the number of levels increases in the hierarchy, the number of attributes grows exponentially making this scheme infeasible on a large scale.

In this paper, a Privilege-based Multilevel Organizational Data-sharing scheme (P-MOD) is proposed. It builds to solve the problems of sharing data within organizations with complex hierarchies. The main contributions presented in this paper can be summarized as follows:

- We present 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.

Advantages:

- We 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.

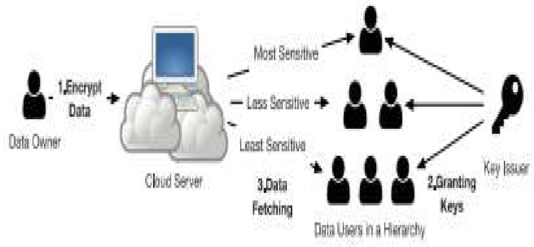


Fig.1: System architecture

- Based on the problem described above, we have the following design goals:
- Privilege-Based Access: Data is shared in a hierarchical manner based on user privileges. Data users with more privileges (ranked at the higher levels of the hierarchy) are granted access to more sensitive parts of F than those with fewer privileges (ranked at the lower levels of the hierarchy).
- Data Confidentiality: All parts of F are completely protected from unprivileged data users (including the storage space). Data users are entitled to access the parts of F corresponding to the levels they fall in and/or any other parts corresponding to the levels below with respect to their own.
- Fine-grained access control: The data owner has the capability to encrypt any part of F using any set of descriptive attributes he/she wishes, limiting access to only authorized data users. The set of descriptive attributes is defined by the data owner at the time of encryption and can be selected from an infinite pool.
- Collusion resistant: Two or more data users at the same/ different level can not combine their private keys to gain access to any part of F they are not authorized to access independently.

4. IMPLEMENTATION

4.1 Modules:

- Data owner
- User
- Key-issuer
- Cloud

4.2 MODULES DESCRIPTION:

DATA OWNER

Data owner is the sole proprietorship of the data. He is responsible for uploading files to the cloud in an encrypted format. He also has full responsibility for the evaluation of the security requirements of the data. File encryption is performed by the data owner and the secret keys are shared between him and the user through their personal official email. Each file is encrypted separately with the attributes of the user. The user who satisfies the access policy are able to download the file from the cloud in its encrypted form.

USER

Persons who request data from the data owner or the organization. They authenticate themselves in the system before accessing the encrypted data from the cloud. Users are able to request and download a file if their attributes much correctly with the ones used to encrypt the file. After users satisfying the access policy, the file requested is sent to their email with the secret key to decrypt. Users can also download the encrypted file from the cloud with ease and decrypt it with the secret key obtain from the data owner.

Key-issuer:

In this module, we develop the Key Issuer module. The key issuer is a fully trusted entity that generates private keys for the data users that possess a correct set of attributes.

CLOUD

The location where encrypted data is stored. The data would be stored in addition to the email address link of the data owner. Cloud provider's responsibility is to provide storage for the encrypted data. They can neither decrypt the file nor change the access policy since keys for encryption and decryption are all maintained by the data owner outside the cloud environment.

5. EXPERIMENTAL RESULTS

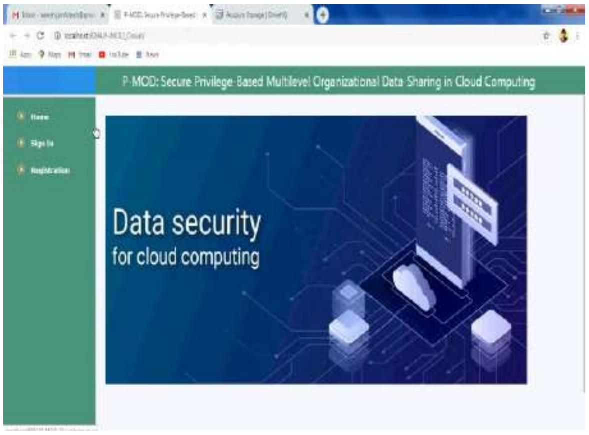

P-MOD: Secure Privilege-Based Multilevel Organizational Data-Sharing in Cloud Computing
Home
Sign In
Registration
Data security
for cloud computing

Fig.2: index

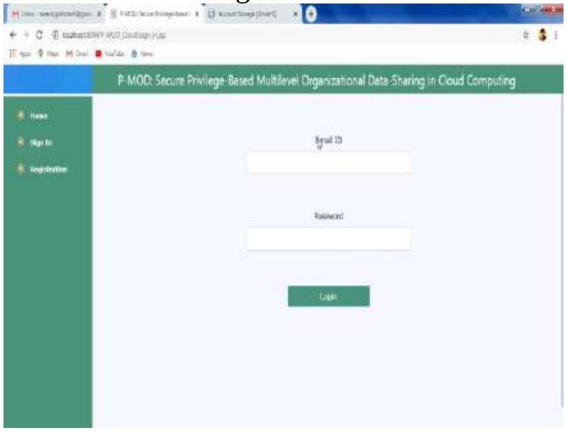

P-MOD: Secure Privilege-Based Multilevel Organizational Data-Sharing in Cloud Computing
Home
Sign In
Registration
Email ID
Password
Login

Fig.3: Login page

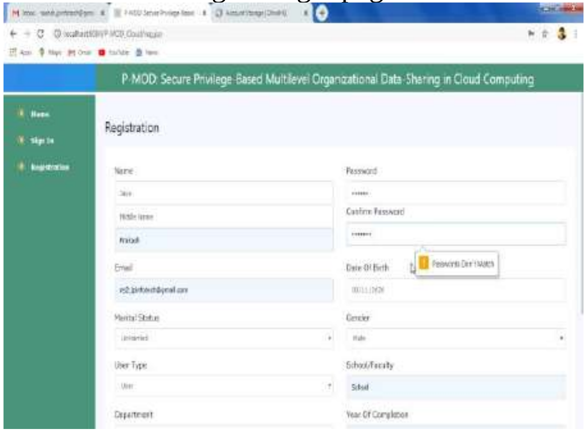
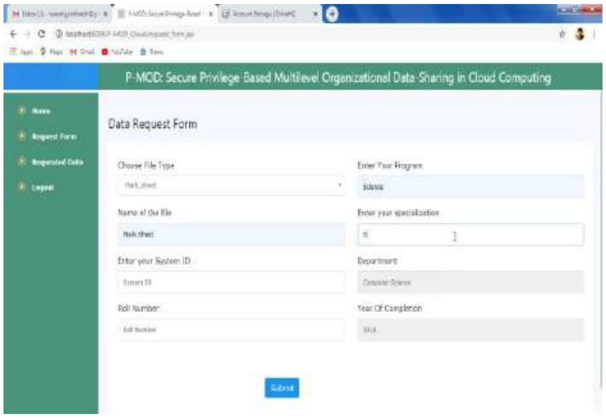


Fig.4: Register



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

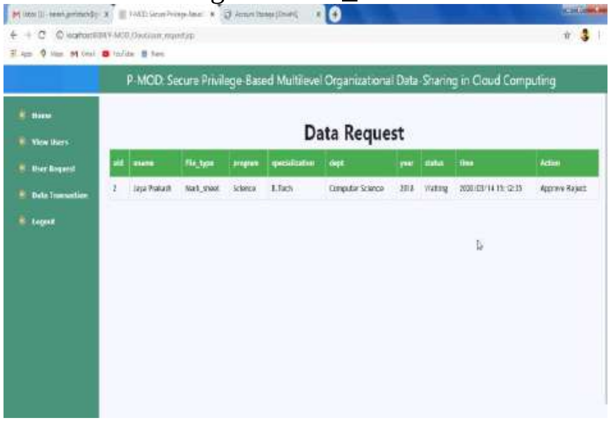
Data Request Form

Choose File Type	Enter Your Program
Mark_sheet	Science
Name of the File	Enter your specialization
Mark sheet	It
Enter your System ID	Department
System ID	Computer Science
Roll Number	Year Of Completion
Roll Number	2018

Fig.5: Request_form

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

Fig.6: Owner_home

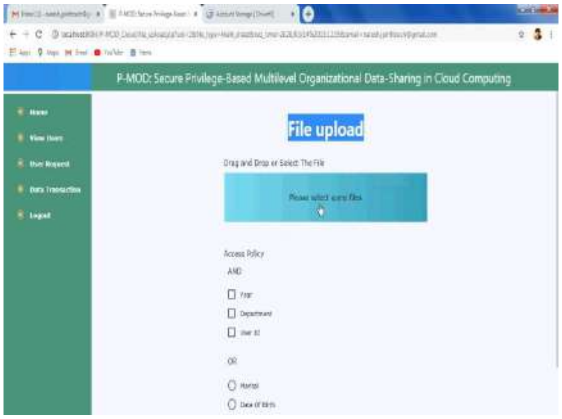


P-MOD: Secure Privilege-Based Multilevel Organizational Data-Sharing in Cloud Computing

Data Request

uid	uname	file_type	program	specialization	dept	year	status	time	Action
2	Jaya Prakash	Mark_sheet	Science	B.Tech	Computer Science	2018	Waiting	2020:03/14 15:12:35	Approve Reject

Fig.7: User_req



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

File upload

Drag and Drop or Select The File

Please select some files

Access Policy

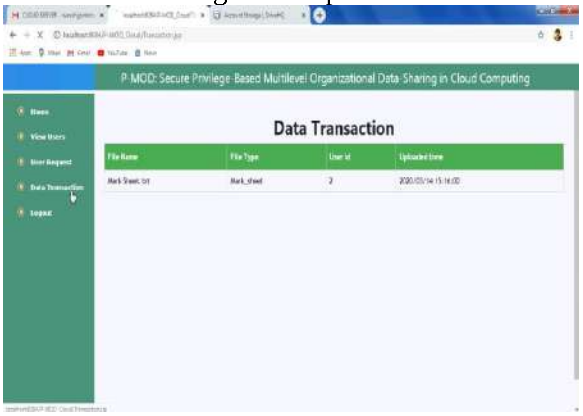
AND

□ Year
□ Department
□ User ID

OR

○ [illegible]
○ Date Of Birth

Fig.8: Fileupload

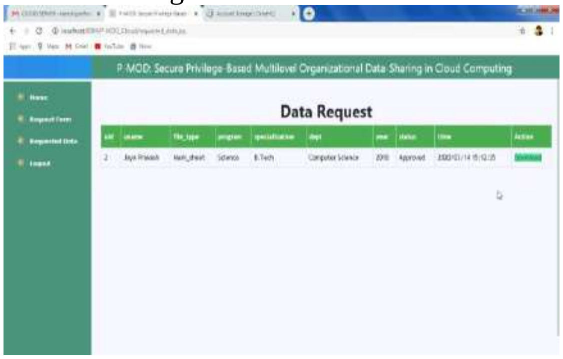


P-MOD: Secure Privilege-Based Multilevel Organizational Data-Sharing in Cloud Computing

Data Transaction

File Name	File Type	User id	Uploaded time
Mark Sheet.txt	Mark_sheet	2	2020/03/14 15:16:00

Fig.9: DataTranscation

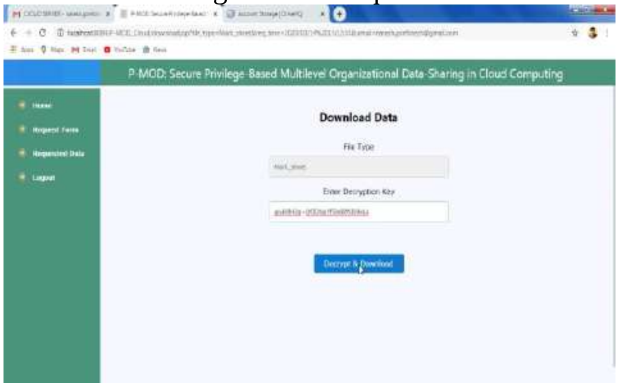


P-MOD: Secure Privilege-Based Multilevel Organizational Data-Sharing in Cloud Computing

Data Request

uid	uname	file_type	program	specialization	dept	year	status	time	Action
2	Jaya Prakash	Mark_sheet	Science	B.Tech	Computer Science	2018	Approved	2020/03/14 15:12:35	Download

Fig.10: Data request



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

Download Data

File Type

Mark_sheet

Enter Decryption Key

[illegible]

Decrypt & Download

Fig.11: Download

6. CONCLUSION

The numerous benefits provided by the cloud have driven many large multilevel organizations to store and share their data on it. 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 Data sharing 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

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

[4] A. C. OConnor and R. J. Loomis, "2010 economic analysis of role-based access control," NIST, Gaithersburg, MD, vol. 20899, 2010.

[5] A. Elliott and S. Knight, "Role explosion: Acknowledging the problem.," in Software Engineering Research and Practice, pp. 349–355, 2010.

[6] 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.

[7] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in 2007 IEEE Symposium on Security and Privacy (SP'07), pp. 321–334, IEEE, 2007.

[8] 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.

[9] 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 Trans. In. Forensics Security, vol. 11, no. 6, pp. 1265–1277, Jun. 2016.

[10] M. Lichman, "UCI machine learning repository," Irvine, CA, 2013.