INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND ENGINEERING TECHNOLOGIES

ISSN : 2454-9924

Secure Privilege-Based Access Structure In Cloud Computing

(R SUNITHA KUMARI) [1] (A SRINIVASAN) [2]

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING,

SIR VISHVESHWARAIAH INSTITUTE OF SCIENCE AND TECHNOLOGY(SVTM)

EMAIL ID: sunitharachapalli @gmail.com

Abstract

As we turn to the cloud for more data storage needs, finding a secure and efficient data access structure has become a serious research problem. We have proposed a Privilege-based Multilevel Organizational Data-Sharing Scheme (P-Mode). We demonstrate multiple file partitioning methods and propose a unique-based access structure that facilitates data sharing in hierarchical settings. This makes it easier for organizations during large data analyzes to comprehensively know the population. Security analysis shows that DBDH umption is safe against plain text attack in favor of uming.

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

INTRODUCTION:

Cloud computing means storing and accessing data and programs online, not just on your computer disk drive. Cloud is usually private or public. General Public Cloud sells services to anyone online. It is often a private cloud-owned network or knowledge hub that provides services hosted by a limited number of people with specific access and permissions settings. Private or public, the goal of cloud computing is to provide easy, scalable access to computing resources and IT services.

One of the main ways in which enormous companies adapt to increased sensitive data management is to use the cloud environment. All U.S. Businesses are reported to have switched to the cloud for his or her business data management needs. On-demand cloud access and data sharing greatly reduce data management cost, storage convenience and efficiency. However, data owners can be seriously concerned when sharing data in the cloud thanks to security issues. After uploading and sharing, the owner of the information Loss of control over information inevitably opens the door to unauthorized data access.

Consider the illustration of patients accessing their Public Health Records (PHR) in the cloud by health providers and hospital administrators. In most cases, the patient wants to be granted access to a physician for most parts of the PHR (including its most sensitive components, e.g., medical history), while the administrator gives access to less sensitive (e.g., date of birth) limited parts. Therefore, the patient should define a range of cognitive rights that rank different types of hospital employees. Next, the patient must specify the powers at each level to define the content that each data user can access. It is important to understand that patients have different conservative beliefs when it comes to their PHRs. For example, some want to grant access only to specific physicians for sensitive parts of their PHRs.

RELATED WORKS:

Blurred Identity-Base Encryption (Blurred IBE) was introduced to manage data sharing in the cloud in a simpler way using encryption. The cipher is shared in the cloud to restrict access to authorized users. Therefore the licensed person must request a private key from the user key-issuer to decrypt the encrypted data, in order to obtain the information. Blurred IBE may be a specific type of function encryption, during which both the private key and the cipher of the information user are associated with the attributes. Properties are detailed pieces of data assigned to any user or object. Since attributes are often any variable, they provide greater flexibility when granting data access. This scheme allows a group of detailed features to be associated with the private key and therefore shared in the ciphertext cloud. If the information user's private key requires a minimum entry of features that match the features incorporated in the cipher, the information user can decrypt it. Although this scheme allows complex systems to be easily defined using features, it is less efficient when larger systems cannot express or increase the amount of features.

Attribute-based encryption (ABE) schemes later emerged to provide more versatility when sharing data. These schemes connect two types of structures: properties and access policies. Accessibility Policies Ads that add features to tell exactly which users of the system have been granted access and which users will be rejected. ABE schemes are introduced through two different approaches, Key-Policy Attribute-Based Encryption (KP ABE) and Ciphertext Policy Attribute-Based Encryption (CP-ABE). In KP-ABE, each cipher is labeled with a set of descriptive features, while each private key is associated with an access policy. Technical Data Users In order to decrypt a cipher, they must first obtain a private key to use in decryption from the person issuing the key. Key-issuer Access the policy into generated keys. Data users can successfully decrypt the cipher if the set of detailed features related to the cipher technology satisfies the access policy incorporated in their private keys. KP-ABE can perform fine-grained access control and is simpler than fuzzy IBE. However, the data owner must trust the key-issuer to issue private keys only to data users who have been granted the right of access. This is often a limitation as the information user eventually loses control over what data users should be granted access to. Hierarchical Attribute-Based Encryption (HABE) and CP-ABE were introduced after the Com hierarchical Identity-Based Encryption (HIBE) scheme. Stay in position time | Ready "> is in a position to perceive good-access control in a hierarchical organization that includes the root master who generates and distributes the keys, multiple domain masters and different users who assign the keys to the" "domain master at the next level. Are generated in a single hierarchical key generation process. To express accessibility, HABE uses a typical general form where all attributes are managed as a conjunctive term from the same domain authority. The scheme becomes inappropriate for practical implementation when replicas of similar features are maintained by other domain authorities. Synchronizing feature administration with complex organizations that have multiple domain executives can become challenging.

File hierarchical ciphertext policy attribute-based encryption (FH-CP-ABE) is one of the first hierarchical solutions available today. It proposes an equalized access structure to maintain a hierarchical organization that shares data of varying sensitivities. An access structure is proposed, which refers to the hierarchy and therefore the access policies of the corporation. This is the 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. 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 ciphertext of highest sensitivity and any other ciphertext with less sensitivity in the lower levels of the hierarchy. The nodes ranked in the lower levels (transport nodes) cannot 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. As a result, storage space is saved as only one copy of the ciphertext is needed to be shared on the cloud for all data users. However, since 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. A simplified and reduced access structure is proposed to reduce the computational complexity by removing all branches of the single access structure while keeping one full branch. The full branch consists of the root node, a set of transport nodes (one for each level), and the leaf nodes (attributes). 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.

METHODOLOGY:

- 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.
- We present 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 U.S. Census Income data set.

ALGORITHM:

A. Cryptographic Hash Function

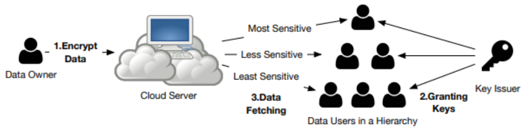
A cryptographic hash function h is a mathematical algorithm that maps data of arbitrary size to a bit string of fixed size. It is cryptographically secure if it satisfies the following requirements:

- Preimage-Resistance: It should be computationally infeasible to find any input for any pre-specified output which hashes to that output, i.e. for any given y, it should be computationally infeasible to find an x such that h(x) = y.
- Week Collision Resistance: For any given x, it should be computationally infeasible to find x 0 6= x such that h(x 0) = h(x).
- Strong Collision-Resistance: It should be computationally infeasible to find any two distinct inputs x and x 0 , such that h(x) = h(x 0).

B. Decisional Bilinear Diffie-Hellman (DBDH) Assumption:

The DBDH assumption is a computational hardness assumption and is defined as follows: Let G0 be a group of prime order p, g be a generator, and a, b, c ∈ Zp be chosen at random. It is infeasible for the adversary to distinguish between any given (g, ga , gb , gc , e(g, g) abc) and (g, ga , gb , gc , R), where R ∈r G1 is a random element and ∈r denotes a random selection. The DBDH assumption holds if no polynomial algorithm has a non-negligible advantage in solving the DBDH problem.

ARCHITECTURE:



CONCLUSION:

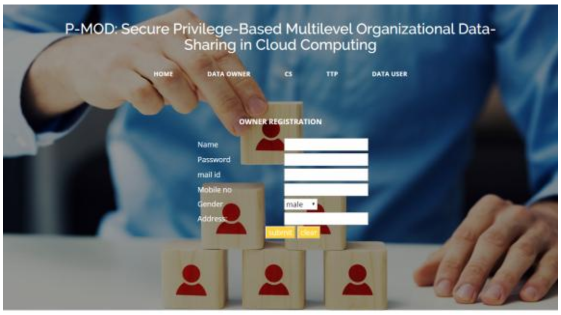
The numerous benefits provided by the cloud have driven many large multilevel organizations to store and share their data on it. This begins by pointing out major security concerns data owners have when sharing their data on the cloud. Next, the most widely implemented and researched data sharing schemes 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.

SCREENSHOTS:

Home_Page

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

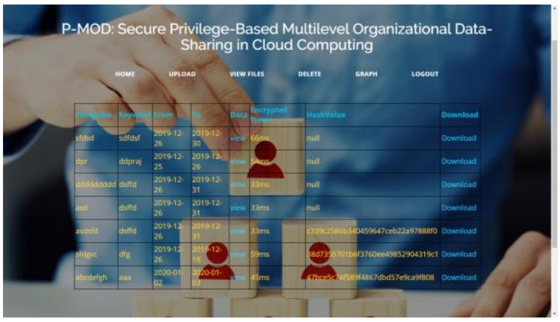
Data_Owner_Registration


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

OWNER REGISTRATION

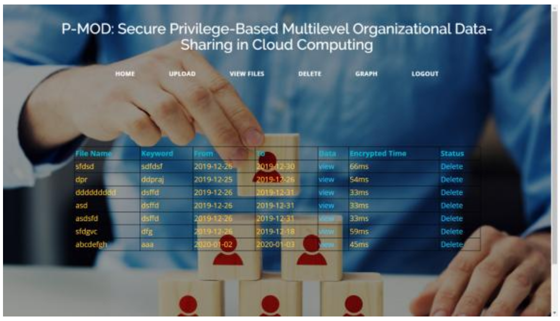
Name
Password
mail id
Mobile no
Gender male
Address

View_Files


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

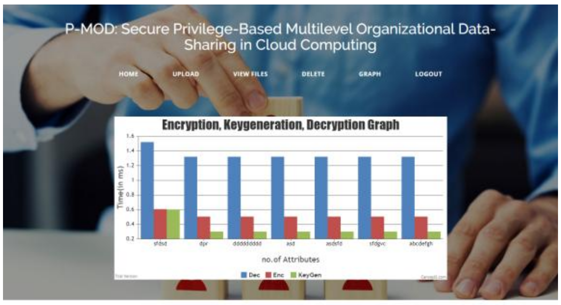
File Name	Keyword	From	To	Data	Encrypted Time	HashValue	Download
sfdsd	sdfdsf	2019-12-26	2019-12-30	view	66ms	null	Download
dpr	ddpraj	2019-12-25	2019-12-26	view	54ms	null	Download
ddddddddd	dsffd	2019-12-26	2019-12-31	view	33ms	null	Download
asd	dsffd	2019-12-26	2019-12-31	view	33ms	null	Download
asdsfd	dsffd	2019-12-26	2019-12-31	view	33ms	c339c2586b340459647ceb22a97888f0	Download
sfdgvc	dfg	2019-12-26	2019-12-18	view	59ms	38d7355701b6f3760ee49852904319c1	Download
abcdefgh	aaa	2020-01-02	2020-01-03	view	45ms	47bce5c74f589f4867dbd57e9ca9f808	Download

Delete_files

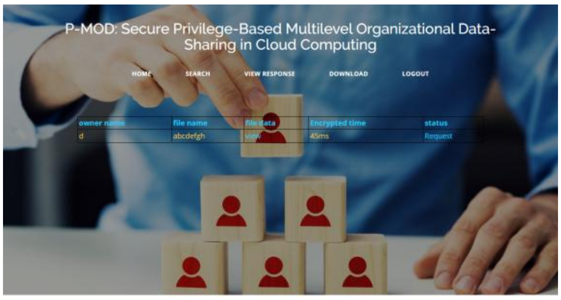

P-MOD: Secure Privilege-Based Multilevel Organizational Data-Sharing in Cloud Computing

File Name	Keyword	From	To	Data	Encrypted Time	Status
sfdsd	sdfdsf	2019-12-26	2019-12-30	view	66ms	Delete
dpr	ddpraj	2019-12-25	2019-12-26	view	54ms	Delete
ddddddddd	dsffd	2019-12-26	2019-12-31	view	33ms	Delete
asd	dsffd	2019-12-26	2019-12-31	view	33ms	Delete
asdsfd	dsffd	2019-12-26	2019-12-31	view	33ms	Delete
sfdgvc	dfg	2019-12-26	2019-12-18	view	59ms	Delete
abcdefgh	aaa	2020-01-02	2020-01-03	view	45ms	Delete

View_Graph

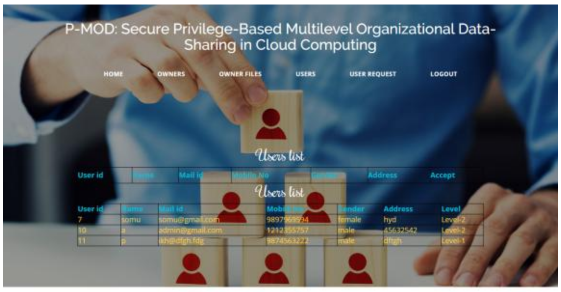

P-MOD: Secure Privilege-Based Multilevel Organizational Data-Sharing in Cloud Computing

View_Files


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

owner name	file name	file data	Encrypted time	status
d	abcdefgh	view	45ms	Request

Data_Users



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

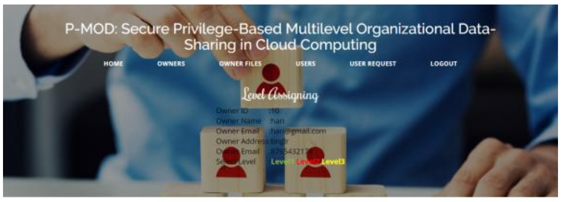
Users list

User id	Name	Mail id	Mobile No	Gender	Address	Accept

Users list

User id	Name	Mail id	Mobile No	Gender	Address	Level
7	somu	somu@gmail.com	9897969594	female	hyd	Level-2
10	a	admin@gmail.com	1212355757	male	45632542	Level-2
11	p	lkh@dfgh.fdg	9874563222	male	dftgh	Level-1

Assign_Levels



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

Level Assigning

Owner ID :10
Owner Name :hari
Owner Email :hari@gmail.com
Owner Address :bndr
Owner Email :9765432178
Select Level Level1 Level2 Level3

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 Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1265–1277, 2016.

[10] M. Lichman, “UCI machine learning repository,” 2013.