ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 12, December 2018

A Survey on Novel Approach for Multi-Authority Attribute-Based Encryption for Data Security

Vikramsinh Rajendra Ghatge, Prashant M. Mane

M. E Student, Department of Computer Science and Engineering, Zeal College of Engineering & Research, Pune, India

Assistant Professor, Department of Computer Science and Engineering, Zeal College of Engineering & Research, Pune, India

ABSTRACT: Multi-authority attribute based encryption used for solving many issues of sharing data on cloud and this system is rely on decentralized authority. And using the Global identifier solve the issue of collusion, so need to manage the identities globally and it creates problem for security. User identities are unique by combining a user’s identity with the identity of the Attribute Authority where the user is located. If the key request wants to be maintain by outside domain, the request to be perform by the authority in current domain rather than by user. And therefore the privacy and security of user identity remain private by attribute authority from outside domain. In the scheme, use de-duplication concept for the purpose of save the lots of memory and don’t provide duplicate file on cloud and improve performance. Integrity of data is checked by attribute authority to reduce the time to get data from the cloud.

KEYWORDS: Attribute authority ,cloud computing, Encryption, privacy preserving

I.INTRODUCTION

I.I. Background:

Attribute-based Encryption (ABE) is an efficient encryption system with Fine-grained access control for encrypting out-sourced data in cloud computing. With the emergence of sharing confidential corporate data on cloud servers, data are generated by several organizations, and access policies can be defined by several authorities. Single-authority ABE cannot meet the demands of decentralized distribution, and decentralizing multi-authority ABE have been proposed to solve those problems. For basic Identity-based encryption (IBE) and ABE, all private keys are managed by an authorized centre. However, in practice, this will present a performance bottle-neck requiring evaluation due to the huge numbers of requests. In basic ABE systems, the information shared is always within one domain or organization. However, in reality, information such as drivers' licenses and registration information in universities are organized by different government departments. The management of attributes and key distributions cannot be undertaken by the same attribute authority. Moreover, access strategies may be distributed based on attributes of different authorities. Therefore, levelled multi-authority ABE cannot meet distribution demands. Decentralizing multi-authority ABE is used to solve the access problem in which user attributes belong to different authorities. Those authorities differ from that for a levelled multi-authorized ABE, for which the levelled multi-authority ABE has one trust root. There is no trust between organizations, and attribute management and key distribution always are performed separately from each other.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 12, December 2018

I.II.MOTIVATION:-

- On cloud identity needs to be managed globally, which results in the crucial problems of privacy and security.
- Single-authority ABE cannot meet the demands of decentralized distribution.
- Identity-based encryption (IBE) and ABE, all
- private keys are managed by an authorized centre. However, in practice, this will present a performance bottle-neck requiring evaluation due to the huge numbers of requests.
- Multi authority ABE use for access the data from cross domain and handle collusions. And also the system is supports for de-duplicate and save memory and time also.

II. REVIEW OF LITERATURE

1]"User collusion avoidance scheme for privacy-preserving decentralized key-policy attribute-based encryption," This paper presents propose a user collusion avoidance scheme which preserves the user's privacy when they interact with multiple authorities to obtain decryption credentials. The proposed scheme mitigates the well-known user collusion security vulnerability found in previous schemes proposed a PP KP-ABE scheme for a distributed data sharing environment. The proposed scheme enables users to download and decrypt the data from online such as cloud without revealing their attributes to the third-parties. The novelty of the work is to mitigate the user collusion attack in the existing scheme[1].

2] "Secure threshold multi authority attribute based encryption without a central authority'"
This paper presents a threshold multi authority fuzzy identity based encryption(MA-FIBE) scheme without a central authority for the first time. An encrypter can encrypt a message. The security proof is based on the secrecy of the underlying joint random secret sharing protocol and joint zero secret sharing protocol and the standard decisional bilinear Diffie-Hellman assumption. The proposed MA-FIBE could be extended to the threshold multi authority attribute based encryption (MA-ABE) scheme and be further extended to a proactive MA-ABE scheme[2].

[3] "The design of an m-health monitoring system based on a cloud computing platform," Present paper, a framework of an m-Health monitoring system based on a cloud computing platform (Cloud-MHMS) is designed to implement pervasive health monitoring. Furthermore, the modules of the framework, which are Cloud Storage and Multiple Tenants Access Control Layer, Healthcare Data Annotation Layer, and Healthcare Data Analysis Layer, are discussed[3].

[4] Fuzzy identity-based encryption," Present two constructions of Fuzzy IBE schemes. Our constructions can be view as an Identity-Based Encryption of a message under several attributes that compose a (fuzzy) identity. Our IBE schemes are both error-tolerant and secure against collusion attacks. Additionally, our basic construction does not use random oracles. System prove the security of our schemes under the Selective-ID security model[4].
[5] "Decentralizing attribute-based encryption.Present construct a Decentralized Ciphertext-Policy Attribute-Based Encryption (DCP-ABE) scheme. Under this scheme, any participating entity can act as an authority by creating a public key. The authority utilizes the users' attributes to generate the private keys for them. Any user can encrypt data in terms of any monotone access structure over attributes issued from any chosen set of authorities. Hence the protocol does not depend on any central authority[5].

[6] "Expressive cp-abe with partially hidden access structures"Present a new model for CP-ABE with partially hidden access structures. In our model, each attribute consists of two parts: an attribute name and its value; if the private key attributes of a user do not satisfy the access structure associated with a ciphertext, the specific attribute values of the access structure are hidden, while other information about the access structure is public[6].

[7] " Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud "Propose a novel multi- keyword fuzzy search scheme by exploiting the locality-sensitivehashing technique. Our proposed scheme achieves fuzzy matching through algorithmic design rather than expanding the index file. It also eliminates the need of a predefined dictionaryand effectively supports multiple keyword fuzzy search [11].

[8] "An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing " Public key encryption algorithm for encrypting the data and invoke ranked keyword search over the encrypted data to retrieve the files from the cloud. Proposed system aim to achieve an efficient system for data encryption without sacrificing the privacy of data. Further, our ranked keyword search greatly improves the system usability by enabling ranking based on relevance score for search result, sends top most relevant files instead of sending all files back, and ensures the file retrieval accuracy[12].

[9] " Privacy preserving multi-keyword text search in the cloud supporting similarity basedranking "Present a privacy-preserving multi-keyword text search (MTS) scheme with similarity-based ranking to address this problem. To support multi-keyword search and search result ranking, Proposed system propose to build the search index based on term frequency and the vector space model with cosine similarity measure to achieve higher search result accuracy[13].

[10.]" Shared and searchable encrypted data for untrusted servers," Journal of Computer Security, "construct a special tree-based index structure and propose a "Greedy Depth-first Search" algorithm to provide efficient multi-keyword ranked search[15].

III.PROPOSED WORK

SYSTEM OVERVIEW-
In the proposed system, the DMA system: AA (Attributes Authority), Cloud storage provider (CSP),PM-Project manager, Employee.

1.**PM(PM)**-Project manager is responsible for defining access policy and encrypting data under the access policy. Furthermore, the company's project manager needs to upload the encrypted data to the remote cloud storage server. At the time file upload on cloud that time data deduplication is performed that will check if previous any file of that data is stored on cloud or not. If present the an indexing will perform and data stored message will display to project manager. For deduplication it uses MD5 Algorithm to check similarity between data.
AA (Attribute Authority)-AA plays the role of attributes distribution and employee authorization. It computes employee' attributes based on the public parameters and distributes them to Project manager and employees for access policy definition. Every AA can manage multiple attributes and has full control over those attributes. To build trust relations, only global parameters and public key information need to be swapped between attribute authorities. Attribute authority will check integrity of his domain's file. If data is loss then he will inform to that file's data owner your file is tempered so he have to upload the file.
Cloud Server Provider (CSP). CSP is considered as a semi-trusted storage media that stores data. The CSP does not have the secret keys, so it can't decrypt the cipher-text. It will see AA ,Project manager and employee details.
Employee. Cipher-text on the cloud server can be accessed freely by employee. But only when the employee's attributes satisfy the access policy that defined in the cipher-text, can he/she decrypt the cipher-text. Employee's attributes are distributed by a number of authorities according to the user privileges so that it can achieve cross-domain access control. Employee can view the file and send the request outside the domain. That request is forwarded by current domain AA to outside domain AA. Then that key will get by current AA and will send to user.

DOI: 10.15680/IJIRCCE.2018. 0612010

IV. PROPOSED SYSTEM ARCHITECTURE

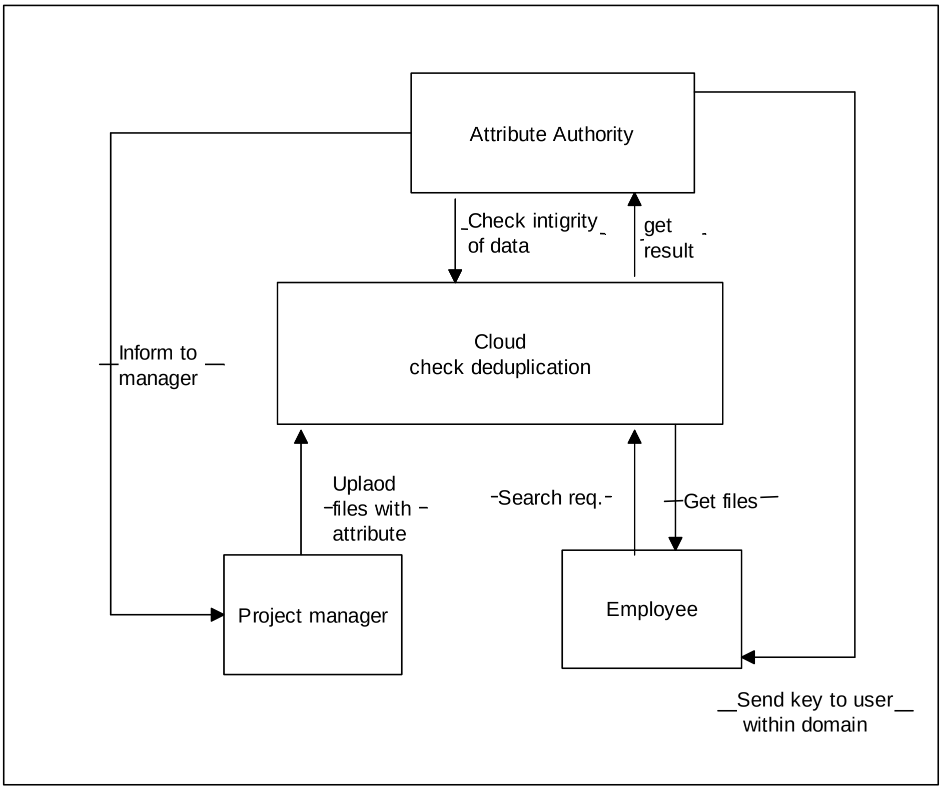

Fig.1: System architecture

Advantages:

1.privacy and security have been enhanced dynamically.
2. User identities tend to be unique globally to achieve collusion resistant, but identities need not be published globally.
3.In proposed system Integrity checking is performed that will reduce more time to access data from the cloud.
4.Data deduplication is performed that will reduce storage space more.It uses MD5 Algorithm to check similarity between data.

V. CONCLUSION

Propose system achieve security by using ABE and IBE algorithm. In ABE uses multi authority ABE, it solve many issues of privacy requirements of sharing data on clouds. Proposed system utilize get to tree that oversee credits which has a place with various specialists to accomplish cross-area data storage and access control. The system achieve cipher text access control, preventing collusion attacks between users and authorities as well as improve the efficiency

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 12, December 2018

of cipher text encryption and decryption. So the proposed system can access data from cross domain with encryption and decryption. Proposed system will work on storage reduction and also on integrity checking of data.

REFERENCES

[1]Y. Rahulamathavan, S. Veluru, J. Han, F. Li, M. Rajarajan, and R. Lu, ``User collusion avoidance scheme for privacy-preserving decentralized key-policy attribute-based encryption," IEEE Trans. Comput., vol. 65, no. 9, pp. 2939_2946, Sep. 2016

[2] H. Lin, Z. Cao, X. Liang, and J. Shao, ``Secure threshold multi authority attribute based encryption without a central authority," in Proc.INDOCRYPT, Kharagpur, India, Dec. 2008, pp. 426_436

[3] B. Xu, L. Xu, H. Cai, L. Jiang, Y. Luo, and Y. Gu, "The design of an m-health monitoring system based on a cloud computing platform," Enterprise Information Systems, vol. 11, no. 1, pp. 17-36, 2017

[4] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology (EUROCRYPT'05), 2005, pp. 557-557

[5] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'11), 2011, pp. 568-588.

[6] J. Lai, R. H. Deng, and Y. Li, "Expressive cp-abe with partially hidden access structures," in Proceedings of ACM Symposium on Information,Computer and Communications Security (ASIACCS'12), 2012, pp. 18.

[7] A. Lewko and B. Waters, ``New techniques for dual system encryption and fully secure HIBE with short ciphertexts," in Proc. TCC, Zurich, Switzerland, Feb. 2010, pp. 455_579.

[8] G. Wang, Q. Liu, and J. Wu, ``Hierarchical attribute-based encryption for _ne-grained access control in cloud storage services," in Proc. CCS, Chicago, Il, USA, Oct. 2010, pp. 735_737.

[9] G. Wang, Q. Liu, J. Wu, and M. Guo, ``Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers," Comput.Secur., vol. 30, no. 5, pp. 320_331, Jul. 2011.

[10] Z. Shen, J. Shu, W. Xue, "Preferred keyword search over encrypted data in cloud computing," in: IWQoS'13, Montreal, Canada, 2013.

[11] B. Wang, S. Yu, W. Lou, Y. Hou, "Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud," in: INFOCOM'14, Toronto, Canada, 2014.

[12] S. Pasupuleti, S. Ramalingam, R. Buyya, "An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing," J NETW COMPUT APPL., vol. 64, pp. 12 – 22, 2016.

[13] W. Sun, B. Wang, N. Cao, H. Li, W. Lou, Y. Hou, H. Li, "Privacy preserving multi-keyword text search in the cloud supporting similarity based ranking," IEEE T Parall Distr., vol. 25, no. 11, pp. 3025 – 3035, 2014.

[14] Z. Xia, X. Wang, X. Sun, Q. Wang, "A secure and dynamic multikeyword ranked search scheme over encrypted cloud data," IEEE T Parall Distr., vol. 27, no. 2, pp. 340 – 352, 2016.

[15] C. Dong, G. Russello, N. Dulay, "Shared and searchable encrypted data for untrusted servers," Journal of Computer Security, vol. 19, no. 3, pp. 367 – 397, 2011.