IJRRECS/November 2016/Volume-4/Issue-11/6629-6634 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

MULTI-AUTHORITY ATTRIBUTE BASED ENCRYPTION USING SEMI-ANONYMITY AND FULLY-ANONYMITY

S.Mounika[1], J.Ramesh Babu[2]

[1]PG Student, Dept of CSE, BVRIT, Narsapur, T.S, India

[2]Assistant Professor, Dept of CSE, BVRIT, Narsapur, T.S, India

ABSTRACT:

In literature many techniques were recommended to preserve the privacy of understanding contents by means of access control. In literature previous works have focused on privacy of understanding contents additionally to buy control, while less focus is created towards privilege control additionally to identity privacy. It provides privilege control method to decentralize central authority to limit leakage of identity and therefore gains semi-anonymity together with plans tolerant against authority compromise. It permit cloud servers to deal with user access legal rights missing of knowing their identity information together with recommended plan's in a position to defend user privacy against every single authority and here partial particulars are revealed. This paper present Multi-Authority Attribute Based Encryption scheme, which is concentrate on user privacy concerns by providing AnonyControl and AnonyControl-Fallow. In this paper AnonyControl decentralizes the central authority to limit the identity leakage and thus achieves semi-anonymity. Consequently, this encryption scheme present the Anonycontrol-F achieve the full anonymity.

Keywords: Access control, Cloud servers, Semi-anonymity, Privilege control, Data contents, Data privacy, Central authority, Anonycontrol.

1. INTRODUCTION:

Cloud computing is an evolving paradigm with tremendous momentum, but its unique aspects exacerbating security and privacy challenges. It has generated significant interest in both academia and industry, but it is still an evolving paradigm. Essentially, it aims at least three challenges. First of all, data confidentiality should be guaranteed. The data privacy is not only about the data contents. Users want to control the data from the hacker or cloud servers, because whenever the sensitive data is outsourced to the cloud servers or another user, at that time user cannot handle the sensitive data in such cases, privacy risks would be raise because the servers or hacker might illegally access sensitive information from the outsourced computation. not only accessing but also the operation should be controlled. Secondly, personal information of each user's is at risk because one's identity is authenticated based on user information for the purpose of privilege control. So the identity privacy also needs to be protected before the cloud enters our life. Finally, the cloud computing system has to be protects from attackers.

2. RELATED WORK:

Various techniques have been proposed to protect the data contents privacy. Identity-based encryption (IBE) was first introduced by Shamir, here an identity is applied on the sender message for the security purpose, so that receiver has to contain matching identity of that message to decrypt it. But here the problem is key can be known to the other authorized user. So that security problems will be rise. Few years later, Fuzzy Identity-Based Encryption is proposed, to use ciphertext with identity as a set overlap key for decryption process. Soon after, more general tree-based ABE schemes, Key-Policy Attribute-Based Encryption (KP-ABE) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) are introduced for simple overlapping. Coming to KP-ABE a user can decrypt the ciphertext if the access tree in his private key is satisfied by the attributes in the ciphertext. When re-encryption occurs again key generator has to re-issue a new private key to access re-encrypted files, so re-issuing new private key process causes implementation problems. This will be overcome by CP-ABE; here private keys are generated based on users attributes. A user can decrypt the ciphertext if his attributes in

the private key satisfy the access tree specified in the ciphertext. In this already issued private keys will never be modified unless the whole system reboot. All these techniques have been concentrating on data contents privacy and the access control, but less attention is given on privilege control and identity privacy. Also the user's identities are disclosed to key generators such that lack of protection to the users identities. For protecting identity information Anonycontrol and Anonycontrol-Fallow is proposing to allow cloud servers to control user's access privileges without knowing their identity information.

3. OBJECTIVE:

Our goal ought to be to obtain a multi-authority cipher-text-policy attribute-based file encryption which guarantees privacy of understanding consumer identity and tolerate compromise attacks on government physiques. And to tolerate the compromise attacks on the authorities or collusion attacks by the authorities.

4. METHODOLOGY:

It provides a privilege control strategies that is semi-anonymous for dealing the issues of understanding privacy. And it additionally provides privacy to user identity inside the existed plan of access control. Our plan attains fine-grained privilege control and identity anonymity, while transporting out privilege control according to user identity information by means of multiple government physiques in cloud system. Contrasting from data confidentiality, less focus was compensated towards protection of user privacy using the interactive techniques. User identity is revealed towards key companies, and corporations provide with private keys utilizing their characteristics [3]. Nevertheless it seems normal that clients wish to maintain their particulars secret given that they still obtain private keys. So that advise privilege control strategies by that's semi-anonymous permitting cloud servers to deal with user access legal rights missing of knowing their identity information [4]. This privilege control method decentralizes central authority to limit leakage of identity and therefore gains semi-anonymity. And furthermore it simplifies the file access control to privilege control, by which legal rights inside the entire methods on cloud data are maintained inside the fine-grained method.

5. AN OVERVIEW OF PROPOSED SCHEME:

Cloud computing is a computing method, where sources can be found dynamically by way of Internet and understanding storage is outsourced acquiring a celebration. Fraxel remedies comes complete with plenty of challenges for example guaranteeing of understanding confidentiality private information is extremely in danger since one's identity is validated according to his data for access control purpose cloud system should be flexible regarding security breach where some a part of technique is compromised by attackers [5]. Hence to assist while using the above stated mentioned challenges offer a privilege control strategies that's semi-anonymous for dealing the problems of understanding privacy but additionally privacy of user identity within the existed plan of access control. Earlier works have focussed on privacy of understanding contents in addition to purchase control, while less focus is produced towards privilege control in addition to identity privacy. The forecasted privilege control technique decentralizes central authority to limit leakage of identity and thus gains semi-anonymity. The suggested plans able to defend user privacy against each and every authority and here partial particulars are revealed. The forecasted plan's tolerant against authority compromise. It simplifies the file access control to privilege control, through which rights within the entire methods on cloud data are maintained within the fine-grained way. By way of multiple government physiques in cloud system, our suggested plan attains fine-grained privilege control and identity anonymity while transporting out privilege control based on user identity information. And imagined semi-honest government physiques within suggested plan assumed as that they're susceptible to not collude with each other this is often a needed assumption within suggested system since each authority's subset of complete characteristics set. Once the information inside the entire government physiques is collected altogether, total attribute volume of key requester is enhanced and thus his identity is revealed towards government physiques. During this sense, the suggested technique is semi-anonymous as partial identity facts are revealed towards each authority, but could achieve full-anonymity and furthermore permit collusion of presidency physiques.

Within our system model, as proven in fig1, you will find four organizations for example Attribute Government physiques, Cloud Server, and Entrepreneurs of understanding and consumers of understanding. You might be data owner and understanding consumer concurrently. Government physiques are imagined to contain authoritative abilities, and they're handled by government offices since a few inside the characteristics partially hold user private data. The whole attribute set is broken into disjoint sets and handled by all of the authority, thus all of the authority is mindful of single a part of characteristics. An Information owner is entity that delegate encoded computer file towards cloud servers who'll contain sufficient storage capacity [6]. Lately elevated to complete up part of data consumers request private keys inside the entire government physiques, and furthermore they don't identify which characteristics are addressed by which government physiques. When data consumers request private keys from government physiques, government physiques make equivalent private key and forward it on their own account. The whole data consumers download encoded documents, but just people whose private keys convince privilege tree holds out operation connected by privilege. The server is designated to cope with surgery and just if user credential is confirmed completely through privilege tree.

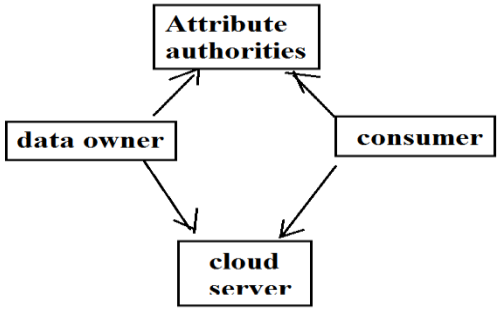

Fig1. Overview of our scheme

6. CONCLUSION:

This paper propose Multi-authority Attribute Based Encryption Scheme which provides a semi-anonymous attribute-based privilege control scheme i.e. AnonyControl and a fully-anonymous attribute-based privilege control scheme i.e. AnonyControl-Fallow to address the user privacy problem in a cloud storage server. The proposed schemes achieved fine-grained privilege control but lack in data contents privacy and access control. More importantly cloud computing system can tolerate up to N-2 authorities. More over multi authorities

mostly concentrated on privilege control and identity privacy.

REFERENCES

[1] M. Chase and S. S. Chow, "Improving privacy and security in multiauthority attribute-based encryption," in CCS. ACM, 2009, pp. 121– 130.

[2] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multi authority attribute based encryption without a central authority," Information Sciences, vol. 180, no. 13, pp. 2618–2632, 2010.

[3] V. Boˇzovi´c, D. Socek, R. Steinwandt, and V. I. Vill´anyi, "Multiauthority attribute-based encryption with honest-but-curious central authority," IJCM, vol. 89, no. 3, pp. 268–283, 2012.

[4] A. Kapadia, P. Tsang, and S. Smith, "Attribute-based publishing with hidden credentials and hidden policies," NDSS, 2007.

[5] S. Yu, K. Ren, and W. Lou, "Attribute-based content distribution with hidden policy," in Workshop on Secure Network Protocols. IEEE, 2008.

[6] Z. Wan, J. Liu, and R. H. Deng, "Hasbe: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing," Information Forensics and Security, IEEE Transactions on, vol. 7, no. 2, pp. 743–754, 2012.