ISSN: 2277-9655
Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

ACCESS PRIVILEGE CONTROL TO PROTECT CLOUD DATA BY USING ANONYMOUS ATTRIBUTE

Dr. Ruksar Fatima*, Aadela Nishat , Prof. Shameem Akhtar
* Department of Computer Science and Engineering, Khaja Banda Nawaz College of Engineering, Kalaburagi, Karnataka, India

DOI: 10.5281/zenodo.50998

ABSTRACT

There are various features which are provided by cloud computing such as pay-as-you-go, availability and use of services with less cost etc. To protect the privacy of cloud content many strategies based on attribute based encryption have been specified.Here we present complete-secrecy right control strategy AnonyControl-F not only for data privacy but for customer identity privacy. AnonyControl-F reaches secrecy by fragmenting the main authority to control the identity leakage. To manage cloud data operations it also branches the file access control to the exemption control. Under the Diffie-Hellman security analysis AnonyControl-F is secure and our accomplishment estimation presents the usefulness of our strategy.

KEYWORDS: Anonymity, multy-authority, attribute-based encryption.

INTRODUCTION

The technique where computing services are provided with the help of internet and also data storage can be done is known as cloud computing. Industries can gain great profit with this technique but there are some issues that need to be solved. First, because user's personal data needs to be protected and no changes should be done by third party or cloud servers, data confidentiality and privilege control should be guaranteed. Second, each individual have their personal information for which some access control is provided to deny access to unauthorized users. As each user is concerned about identity privacy so it should also be protected. Lastly, the cloud system guarantee to recover information when security breach occurs due to attackers.

There are different techniques introduced for data content privacy.One such technique is Identity based encryption [1] where data sent by sender can only be decrypted by receivers having matching identity elements. Next, attribute based encryption or fuzzy identity based encryption [2] was proposed where identity of users is stored as a set of elements and it can be decoded if identity of decrypter has some matching elements with that of its cipher text. Later, Key-Policy Attribute-Based Encryption (KP-ABE) [3] and Cipher text-Policy Attribute-Based Encryption (CP-ABE) [4] are proposed which are tree based ABE schemes where there are conditions that which party can or cannot decrypt the cipher text. In KPABE set of elements are related to cipher text and some unconditional access structures are related with private key to specify user's identity, the user is able to decode the cipher text when the access tree in user's private key matches the elements of cipher text . The encrypter by itself cannot have complete control over encryption because the policy requires private keys too so encrypter needs to trust key generators that he will issue the private keys only to verified users. Whenever re-encryption occurs all customers of same system have to take their keys again to gain access to re-encrypted data. Because of this, different implementation problems occur.

To solve above problems CPABE is presented in which cipher text is associated with access tree to describe who can encrypt or decrypt the data, and private keys are implemented with user's elements. He can only decrypt the

cipher text If elements of user's private key matches the access structure in cipher text. Then only encrypter has the authority for encryption policy and until system's reboot, previously issued private keys will never be modified. While using those protocols, less attention is paid to identity privacy. Identities of users are exposed to key issuers and then issuers can issue those private keys depending on their elements. But its natural that each user wants to keep their identities private. Hence we present here AnonyControl-F through which we can allow cloud servers to control access privilege of user's by keeping their identity information private. It has following advantages:

1. We first accomplish actual toolbox for AnonyControl-F multi authority based encryption.
2. This strategy supports authority accommodation because up to (N-2) accommodation cannot bring the complete system down.
3. To keep individual's information secure from each single authority, AnonyControl-F does not disclose any information.
4. Analysis on security and performance is provided to present feasibility of our strategy.

RELATED WORK

For elegant access control of distributed data cipher text policy based encryption is a favorable cryptographic fundamental. Each customer in CPABE is related to a set of elements and data is encoded with access structures on those elements. A customer can decode the cipher text if his elements match the cipher text content. In [1] authors have focused on important problems of element repudiation which is complex for CPABE. They have resolved this problem with the help of semi secure available online proxy servers. This system allows the authority to reverse customer elements with minimum endeavor. By adversely uniting the technique of proxy re-encryption with CPABE and by allowing the authority to assigning most of heavy tasks to proxy servers they have reached to this solution. The analysis shows that this scheme is secure for the cipher text attacks and this strategy as also applicable for KPABE.

In [2] authors used this strategy where each customer's decryption key is bind with the set of elements showing that customer's liberty. The Customers who have relevant elements to that of encrypted cipher text can decrypt the protected data like only employees with elements such as Human Resources union Executive can decrypt the cipher text on websites. The private keys are bind together with employee's different elements and executive employee's distinct elements. Both of them could decode all the encoded data together. CPABE does not need a any type of storage or secure authority. This Encryption also present as RBAC technique.

In [3] authors described how to split data content into n parts in such a way that those content can easily again structured into the same form by using any k parts and even information about k-1 parts cannot reveal complete information of all data content. This strategy allows the implementation of resilient key management strategy for cryptography which can work firmly and accurately even when adversity damage some of the parts and security issues disclose one of remaining parts.

Most of the personal information is being stored on cloud because cloud computing is becoming more general so private data needs to be encoded before storing it to make it secure. Traditional methods only support Boolean search with the encoded data keywords but it has 2 disadvantages. First, the customers have to perform operations in order to find content matched with their interest. On the other hand, regularly accessing all files may increase unwanted network traffic. In [4] authors present securely organized keyword search over encoded data cloud. This search increases the system usability by giving back matched files in a ranked order, which keeps data privacy in cloud computing. First they present the ranked keyword search with Searchable Symmetric Encryption (SSE) by revealing its inefficiency. Then they present its proper design by using existing cryptographic resources i.e. Order Preserving Symmetric Encryption (OPSE). The analysis shows this technique is much secure than SSE and also demonstrate its efficiency.

Users can store their data remotely on cloud because of its features like pay-as-you-go and access of services from anywhere. With the help of data distribution quality the users can avoid data storage and maintenance operations. For users with limited resources the process of data integrity protection on cloud became very challenging. When users need to check their data integrity they can rely on an external audit party to keep cloud data storage secure. Two basic needs to present Third Party Auditor (TPA) are 1) It should perform data analysis without requesting the

ISSN: 2277-9655
Impact Factor: 3.785

local data copy and 2) It should not bring new problems for data protection. In [5] authors proposed privacy preserving public cloud similar valuator with stochastic covering. Although this scheme is very secure. To increase the main result into multi user setting they have used the functionally assembled signature where third party auditor can perform multiple verifications simultaneously. Individual fitness series (IFS) is an increasing model for health information exchange, which is sometimes stored at third party like cloud providers. Due to exposure of individual health information to third party servers and unapproved parties the privacy problems are increasing. It is a feasible method to encrypt the IFS before taking it on to surely control the patient's access over their IFS. The risks like adaptive access, useful customer repudiation and privacy hazards have remained the important challenges for achieving data access control cryptographically. In [6] authors proposed a framework for patients to access the IFS data stored at semi secure servers. To encrypt individual patient's IFS file they dominate attribute based encryption for breakable and flexible data access of IFS. They have focused on providing data to multiple owners and categorized the customers into different security areas which minimize the key management sophistication for customers and owners. Achieving greater patient privacy while gaining multi authority attribute based encryption has been guaranteed. This strategy also supports continuous change of access protocols and files attributes and required customer repudiation. Substantial results present the security, feasibility, and usefulness of this strategy.

EXISTING SYSTEM

Various procedures have been proposed to ensure the information substance security by means of access control. [1] Identity-based encryption (IBE) was initially presented by Shamir, in which the sender of a message can specify an identity such that only a receiver with coordinating identity can decrypt it. Few years after the fact, Fuzzy Identity-Based Encryption is proposed, which is also known as Attribute-Based Encryption (ABE) [2]. Where the identity of user is represented as the set of attributes and the decryption can only be done if the decoder's identity attributes have some matching with the particular cipher text. The work by Lewko *et al.* and Muller *et al.* [7] are the most comparative ones to our own in that they also attempted to decentralize the central authority in the CP-ABE into numerous ones. Lewko *et al.* utilizes a LSSS framework as an access structure, however their scheme just converts the AND, OR gates to the LSSS matrix, which restricts their encryption policy to boolean formula, while we acquire the adaptability of the access tree having limited gates. Various attribute based strategies for encryption has been proposed with multiple authorities but they use semi secure central authority [8]-[10] and are unable to protect from collision attacks. Muller *et al.* likewise only have Disjunctive Normal Form (DNF) in their encryption policy. The Problems with these are:

1. The identity is validated based on user's data for the reason of access control (or privilege control).
2. Ideally, any authority or server alone should not know any customers personal data.
3. The users in the same framework must have their private keys re-issued in order to access to the re-encrypted documents, and this procedure causes impressive issues in implementation.

PROPOSED SYSTEM

For data confidentiality, less effort is paid to protect users' identity security during interactive protocols. Customer's identities, which are depicted with their properties, are generally disclosed to key issuers, and the issuers issue private keys as indicated by their properties.

We propose AnonyControl-F to allow cloud servers to control customer's access privileges without knowing their identity data. In this setting, every authority knows just a part of any customer's properties, which are insufficient to make sense of the customer's identity. The scheme proposed Considers the essential CP-ABE. There are 4 types of entities: *N Attribute Authorities* (signified as *A*), *Cloud Server*, *Data Owners* and *Data Consumers*. A customer can be a Data Owner and a Data Consumer at the same time. Authorities are expected to have capable calculation capacities, and they are administered by government offices since few properties are incompletely containing customer's identifiable data. The whole property set is divided into N is joint sets and controlled by every authority, in this way every authority is aware of few parts of the properties.

Advantages of Proposed System**:**

1. The user's security is protected by using *AnonyControl-F* strategy where no data is disclosed.
2. The proposed schemes are tolerant against authority compromise, and compromising of up to $(N-2)$ authorities does not bring the entire framework down.
3. We provide detailed investigation on security and execution to show the possibility of the scheme *AnonyControl-F*.

ISSN: 2277-9655
Impact Factor: 3.785

4. We primarily execute *AnonyControl-F* the real toolbox of a multi authority based encryption scheme.

SYSTEM ARCHITECTURE

The architecture Consist of four parties which are Data Owner – which owns data or it is also called as service provider, Data Consumer – which needs access to data also known as user, Trusted Authorities – the authority which provides data and Cloud Servers – servers where user data is stored.
Fig [1] demonstrates System Architecture which consists of 4 steps:

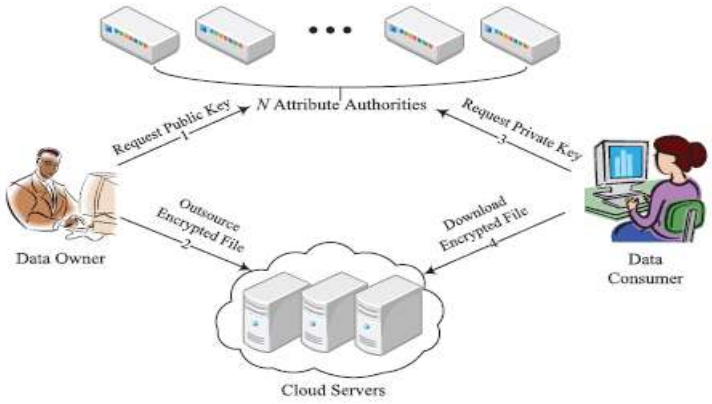

Fig.1 General Flow of Scheme

1. Data Owner first request for the public key from N Attribute Authorities.
2. After getting public key Data Owner outsources the encrypted data or file to the Cloud Sever.
3. The user or Data Consumer then requests for private key to the Trusted Authority.
4. When User receives private key from Authority after authorization of user's identity, He can then download the encrypted data files from Cloud Servers.

METHODOLOGY

The following steps are used to perform encryption and decryption on a file.
1. For a specified algorithm generate a key for a given array of bytes.
2. Generate a cipher text for a specified algorithm.
3. For encryption and decryption initialize the cipher text.

Algorithm

Algorithm 1. Anonymous security using AES and DES methodology. Compute n = pq.

1) Compute (n) = (p − 1)(q − 1) = n − (p + q − 1),
2) Select an integer e where 1 < e < (n) and gcd(e, (n))
3) = 1; i.e., e is coprime.
4) Calculate d as $d \equiv e^{-1} \pmod{(n)}$;
5) $d \cdot e \equiv 1 \pmod{(n)}$
6) e is released as the public key exponent.
7) d is kept as the private key exponent.
8) The public key includes mod n and the public (encryption)
9) Exponent e. The private key includes mod n and the private
10) (Decryption) exponent d, and should be kept secret. p, q,
11) And (n) should also be kept secret as they are used to find
12) The value of d.

algorithm includes 4 steps: key generation, key distribution, encryption and decryption. The algorithm includes

a *public key* and a *private key*.

Key distribution: In key distribution mechanism the users has to send their public key as (n, e) in order to send their encrypted messages. But private key is not distributed. If Alice is sending message to Bob, then, Alice should generate a cipher text using his public key, where as Bob can decrypt the message using her private key, hence Alice's public kley is known to all.

Encryption: Consider a message M that is to be transmitted between 2 users Alice and Bob. Firstly we need to calculate the integer value of M as m and find gcd (*m*, *n*) =1. Then generate the cipher text c for the given message m by using the corresponding users public key.

Decryption: The user Alice can regenerate m from c by applying their respective private key as exponent of d. For *m*, she can regenerate the original message *M* by reversing the padding scheme.

Key generation: The keys in this algorithm are calculated in the following manner: Select at random any 2 prime numbers such as p and q.

CONCLUSION

This proposes AnonyControl-F which is completely unknown attribute-based privilege control mechanism to address the customers security problem in a cloud storage server. Utilizing different authorities in the cloud computing framework, our proposed method accomplish fine-grained privilege control and also identity anonymity while conducting privilege control based on customers identity data. Essentially, our framework can tolerate up to N −2 authority compromise, which is highly better mainly in Internet-based cloud computing environment. A detailed security and performance analysis is conducted which demonstrates that AnonyControl-F both secure and efficient for cloud storage system. The AnonyControl-F directly gets the security but extra communication overhead is incurred during the transfer of selected attributes.

REFERENCES

[1] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in Proc. 5th ASIACCS, 2010, pp. 261–270.

[2] Ciphertext-Policy Attribute-Based Encryption Toolkit. [Online]. Available: http://acsc.csl.sri.com/cpabe/, accessed 2014.

[3] A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.

[4] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Proc. IEEE 30th ICDCS, Jun. 2010, pp. 253–262.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public Auditing for data storage security in cloud computing," in Proc. IEEE INFOCOM, Mar. 2010, pp. 1–9.

[6] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute based encryption," IEEE Trans. Parallel Distributed System., vol. 24, no. 1, pp. 131–143, Jan. 2013.

[7] S. Müller, S. Katzenbeisser, and C. Eckert, "On multi-authority ciphertext-policy attribute-based encryption," Bull. Korean Math. Soc., vol. 46, no. 4, pp. 803–819, 2009.

[8] V. Božovi´c, D. Socek, R. Steinwandt, and V. I. Villányi, "Multi-authority attribute-based encryption with honest-but-curious central authority," Int. J. Comput. Math., vol. 89, no. 3, pp. 268–283, 2012.

[9] F. Li, Y. Rahulamathavan, M. Rajarajan, and R. C.-W. Phan, "Low complexity multi-authority attribute based encryption scheme for mobile cloud computing," in Proc. IEEE 7th SOSE, Mar. 2013, pp. 573–577.

[10] K. Yang, X. Jia, K. Ren, and B. Zhang, "DAC-MACS: Effective data access control for multi-authority cloud storage systems," in Proc. IEEE INFOCOM, Apr. 2013, pp. 2895–2903.