Aspect of join ingress authority for civic directory

S Rajaprakash, S Muthuselvan, C Bagath Basha, A Kesshika, and E Pavithra

Department of Computer Science and Engineering, Aarupadai Veedu Institute of Technology, Vinayaka Mission's Research Foundation, Chennai, Tamil Nadu, India.

Email: kesshikaraji2910@gmail.com

Abstract. Nowadays, Cloud computing is a major and emerging platform that provides various IT related services. The two major factors which inhibit the growth of cloud computing are privacy and security. Hackers can break into public or private cloud environment and steal the data. They can use it with malicious intent such as either use or sell the sensitive information obtained from the business cloud environment. Hence, user's safety depends upon security level in cloud service providers. For an enterprise, there are enormous amount of data is stored and most of them are sensitive information which can affect huge number of people or an entire business organization. Networks are the medium through which all tasks are performed. For access control, being one of the classic research topics, various schemes have been proposed and implemented. In existing key policy, when the key which provides access to the data falls into the wrong hands, they can use it with malicious intent such as steal or alter the data or sell the sensitive information obtained from the business cloud environment. Using our proposed algorithm, we can able to provide a collaborative access control scheme for public cloud storage. This system is implemented using encryption method called Attribute Based Encryption. Encrypting data ensures that even if the data falls into the wrong hands, it is useless as long as its keys remain secure. Even when the hacker gets access to the key, he cannot access the data as only the assigned users can access the data using the key.

Keywords: Attribute Based Encryption, Cipher-Text, Cloud Computing, Computing, Collaborative, Key Encryption.

1. Introduction
This Secure Computing is also known as computer security. Computer security is the protection of computer system and information from harm, theft and unauthorized use. It is the process of preventing and detecting unauthorized use of one computer system. Security of computer means securing a standalone machine by keeping it updated and patched. And it can also be defined as controls that are put in place to provide confidentiality, solidarity and availability for all the components of computer systems. Computer Security is majorly concerned with four important areas: 1. Confidentiality: only authorized users can access the data when needed. 2. Solidarity: only authorized users must be able to modify the data whenever needed. 3. Availability: data should be available to all the users when needed. 4. Authentication: Whether you are really communicating with whom you think you are communicating with. Sensitive data present in ones computer can be misused by the intruder. An intruder can steal, alter or completely modify the source code or sell the sensitive data obtained from the computer. They can also create misleading and offending social accounts which can affect many people. Data theft prevention is absolutely necessary in today's communication networks as most of our everyday actions depends upon the data path security. Data thefts includes theft of account numbers, passwords, credit card info, pins, work related documents etc... Cloud
Cloud computing is the delivery of various services through the Internet (cloud). These resources include tools and applications such as data storage, servers, database, networking and also software. Cloud computing is a in demand option for business people for various reasons including cost savings, increased productivity, speed and efficiency, performance, and security. Many advantages, such as speed and efficiency, via dynamic scaling are provided by cloud computing. But in cloud computing there are also a host of potential threats. These cloud security threats include human error, account hijacking, malicious insiders, data breaches, and DDoS attacks. With increasing in cyber threats across the internet for cloud computing, We need to provide more advanced security to safeguard our data. Cloud computing is an advancement of other web services like web hosting and online storage, and so it faces many of the same risks and from hackers and cyber thieves. Hackers who can break into a private or public cloud computing environment can steal sensitive information from many different types of users and either sell or use that information. Information such a credit card numbers, financial records, software, and reports are stored online by many users and are constantly at risk of being stolen. Cloud service providers (CSP’s), therefore, are obligated to stay vigilant to keep this information safe continually; consequently, user data safety depends on a Cloud Service Providers safety level and culture. Even if that data falls into the wrong hands, Encrypting data ensures that it is useless as long as its keys remain secure. This is beneficial especially when data is being stored in the cloud, as it protects data contents, if a provider, account, or system is compromised.

2. Literature review

The incentive of our work can be dated back to the access control of data stored in untrustworthy servers and collaborative access control. To address access control for data stored in distrustful servers, many works using crypto-graphic and collaborative technologies have been proposed. John Bethencourt, Amit Sahai, Brent Waters introduced ciphertext policy in their work Ciphertext-Policy Attribute-Based Encryption. In their work they described a ciphertext policy attribute-based encryption that we usually describe as a system for encrypted data for complex access control realization. Even when the server is distrustful, using their proposed work, the data encrypted can be confidentially stored. [1] This proposed presents within the cloud, to the media an attribute-based accessibility where which it makes use of ciphertext-policy attribute based encryption (CP-ABE) to assign a key to each and every user attribute by the associate access management and encrypts the data provided by the server. The distributed keys are often encrypted according to the system. [2] This paper proposed an efficient ciphertext policy attribute-based encryption scheme with less computation overhead in the encryption process by providing the short ciphertext and reducing the decryption time by minimizing the pairing operations. Through the security analysis they also demonstrated that their design is secure under chosen-plaintext attack and user collusion attack. [3] Their proposed cryptosystem is seamless to the revocation of user. The security and efficiency of their proposed crypto system had been reported and analyzed. Moreover they implemented the cryptosystem in Charm to demo its practicality. [4] In their proposed work, an advanced key encryption method called symmetric key encryption is introduced. Instead of using usual binary secret keys, images are used as secret keys in their proposed work. Hence, here password letters are converted into a 8 bit binary codes. The pixel values in the image or picture are scanned for the 8-bit codes subsequently represented by the same 8 bit codes. [5] In this proposed system multi authority hierarchical attribute-based encryption & it was compared with the cipher text and key policy attribute based encryption techniques. [6] In this proposed system, they presented the enhancement of a lightweight KP-ABE scheme designed for the Internet of Things. The KP-ABE schemes was claimed to achieve the cipher text in distinguish ability under the chosen-plain text attack in the selective-set model but they showed that the KP-ABE scheme is insecure. [12] SRB18 is mainly discuss about the protection of the twitter analysed data.

Storing a massive number of data in the cloud may pose severe challenges of information theft and data manipulation since all the data is always online, and this leads to a significant problem as its data could be altered for the harmful causes. In the present system, the attribute-based encryption technique, the cloud will not allow collaborative access control for the data users, which can make it less efficient. Attribute based encryption polices are usually associated with data. Also, the attributes
are associated with the keys and particularly those keys which the associated attributes comply can be able to decrypt the data. The existing application is just concentrated on security in the cloud. It focuses on providing access to the high threshold users in the system. And does not provides full hiding of data with other users. In this existing system, the algorithm only concentrates on the accessibility and security methods, which even less protects sensitive data from unauthorized access.

**Gap Identification:**
- A controlled collaborative access scheme is not available in the existing system.
- Sensitive data from the public cloud cannot be safely shared with the low threshold level data users.
- The data owners of the system cannot assign selected users to collaborate and access the data.

### 3. Proposed work

In this proposed system, unlike the standard attribute-based encryption, we let users within the same group to collaborate for data access. The data owner who uploads the data can devise the way for chosen users to combine their attribute sets with satisfying the access policy, and at the same time, also resist the collusion attack when curious users try to combine their attribute sets in other ways.

Technically, we embed translation keys in the secret keys of Ciphertext-Policy Attribute-Based Encryption (CP-ABE) schemes and modify the secret keys to associate groups to all users. The data owner can designate collaboration by setting translation nodes in the policy tree. Our system is highly promising to provide fine-grained access control in collaborative settings where data need to be accessed by multiple users. In the proposed system, the algorithm also concentrates on the accessibility and sophisticated security methods, which even more protects sensitive data from unauthorized access.

#### Advantages
- The controlled collaboration within the same group can be implemented.
- Key privacy will be more secure than the typical attribute based encryption.
- Data is more secure and accessible.
- User collusion resistance is available in the system.

### 4. Methodology

A relatively advanced approach that re-examine the public key cryptography concept called Attribute-Based Encryption (ABE). Many number of cloud storage encryption concepts have been proposed to secure the data from those that have malicious intent and those that don’t have access to the data, for privacy and security reason. All such schemes assumes that the cloud storage providers are heavily secure and cannot be hacked. Even though in practice, some authorities could possibly compel the cloud storage providers to form public user confidentiality and data confidentiality.

In conventional public key cryptography, the receiver’s public key is used to encrypt the message for a specific receiver. The most popular understanding of public key cryptography by allowing a public key to be an arbitrary string such as email address of the receiver is changed by the Identity based Cryptography and in specific Identity Based Encryption (IBE). Attribute-Based Encryption (ABE) goes another step and defines the identity as a set of attributes and not as atomic. For example, with respect to subsets of attributes (key-policy Attribute Based Encryption) or policies that are defined over a set of attributes (ciphertext policy Attribute Based Encryption), roles and messages can be encrypted. The major issue is that a ciphertext can be decrypted only if the user has a key for ‘matching attributes’ same as the trustful person that usually issues the user keys. Attribute Based Encryption (ABE) is a type of public-key encryption where the user’s secret key and the ciphertext are usually relayed upon the attributes. Hence, in such system, only when the set of attributes of the secret key of a user matches the set of attributes of the ciphertext, ciphertext decryption is possible.

#### 5. Performance analysis

A relatively advanced The private key of the users is correlated with a (S) set of attributes in Ciphertext Policy Attribute Based Encryption. Also, in CP-ABE, the access policy atop a defined set
of universe of attributes is specified by the ciphertext policy in confines of the system. The ciphertext can also be able to decrypt by the user, if and only if the attributes satisfies the corresponding ciphertext policy. The policies are usually defined over the attributes using conjunctions, disjunctions and \((k,n)\) threshold gates.

Let us assume that \{P,Q,R,S\} is considered as the universe of attributes. Then, \{P,Q\} be the key to attributes received by the user A. Also \{S\} be the key to attributes received by the user B. Let’s assume that a ciphertext is encrypted according to the \((P \land R) \lor S\) policy. In this case, user B can able to decrypt the ciphertext and user A cannot be able to decrypt. In CP-ABE, authorization is confined into the data that are encrypted and the data can be decrypt by only those people who satisfy the connected policy. Hence, Ciphertext Policy Attribute Based Encryption allows to realize the implied authorization. Additional feature is that once the data had been encrypted corresponding to the policies, the private keys can be obtained by their corresponding users. So, even without the standard set of users, the data can be able to be encrypted. But can only the state the policy which allows decryption. With respect to attributes further users will be given access to key such a way that the policy can be contented can then be able to decrypt the data.

A ciphertext-policy attribute-based encryption scheme is comprised of following four algorithms: Setup, Encrypt, and Key Gen & Decrypt.

Setup \((\lambda, \mathbb{U})\): Attribute universe description and security parameter are taken as input in the setup algorithm. Master key (MK) and the public parameter (PK) are the outputs.

Encrypt \((PK, M, A)\): Encrypt \((PK, M, A)\): Public parameters as PK, a message as M and an access structure as A are taken as input by encryption algorithm over the universe of attributes. This algorithm will encrypt a message (M) & produce a ciphertext (CT) in such a way that a set of attributes owned by only those users can satisfy the access structure (A) can be able to decrypt the M. Its assumed that the ciphertext possibly contain the access structure (A).

Key Generation \((MK, S)\): Master key as MK and set of attributes as S that defines the key are taken as input by the key generation algorithm. Private Key (SK) is taken as output.

Decrypt \((PK, CT, SK)\): Public parameters (PK), a ciphertext (CT) which contains the access policy and SK (Private Key) which is a private key for set (S) of attributes are taken as input by the decryption algorithm. When the Access Structure (A) is satisfied by the (S) set of attributes then ciphertext are bound to decrypted using the algorithm and a message (M) is returned.

### Table 1. Civic Data

| Employee Name | Employee Id | Employee Number |
|---------------|-------------|-----------------|
| Ashok         | 35016135832 | 9381319497      |
| Vijay         | 35016123443 | 8794561937      |
| Priya         | 35016135829 | 9376811956      |
| Karthic       | 35016136591 | 7193561997      |

Decryption algorithm is referred from Somasundaram, Rajaprakash and Bagathbasha21 i.e. “Securing twitter data using srb21 phase 1 methodology”

Phase I: The SRB21 methodology consists of three major steps.
Step 01: From the Civic directory data are extracted as shown in table 1.
Step 02: Analyzed civic data are stored in the matrix K.
Step 03: Using this operation the secret key and prime number secret key of the matrix are exchanged.

\[ S = (n,R) \]
\[ where \quad R = n^{102} - n + K, \]
\[ n \geq 3 \]
\[ if \quad R > N \quad then \]
\[ R_1 = R - N \]
\[ if \quad R_1 > N \quad then \]
\[ R_2 = Add\; R_1\; Digit\; Numbers \]
\[ if \quad R_2 > N \quad then \]
\[ R_3 = Add\; R_2\; Digit\; Numbers \]
\[ if \quad R_3 > N \quad then \]
\[ \text{swap}(n,R_3) \]
\[ \text{break} \]
\[ \text{else} \]
\[ \text{swap}(n,R_2) \]
\[ \text{else} \]
\[ \text{swap}(n,R_1) \]
\[ \text{else} \]
\[ \text{swap}(n,R) \]
\[ if \quad R \mod 2 \neq 0 \quad \&\& \quad R \mod 3 \neq 0 \]
\[ R \mod 5 \neq 0 \quad \&\& \quad R \mod 7 \neq 0 \quad then \]
\[ n = n + 1 \]
\[ \text{else} \]
\[ STOP \]

**Module Description**

**Employee Login:** In this module, employee can login using registered username or employee name and password. Another option for new registration is also provided.

**Admin Login:** Admin is the key administrator for managing all the user or employee accounts. Admin is logged in using registered username and password.

**Registration form:** A new employee is added into the employee portal using employee registration form. Employee’s primary details are submitted in this registration form.

**View employee:** In this module, details of the employee can be viewed. Employee details such as emp name, company name, age, dob, contact no etc. are included.

**Manager login form:** Managers of the two companies responsible for employees are logged in using this module.

**Client registration form:** In this module, client id is registered by giving data such as id, name, company name, email and contact no.

**Manager registration form:** Likewise, manager id is also registered in this module. The proposed system, unlike the standard attribute-based encryption, we let users within the same group to collaborate for data access. The data owner though a conclusion may review the main points of the paper, does not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions. Authors are strongly encouraged not to
call out multiple figures or tables in the conclusion—these should be referenced in the body of the paper.

7. Discussion & conclusion
The proposed Attribute Based Encryption algorithm is a real time system framework. Using a simulator the proposed ABE algorithm has to verify and validate the user. The proposed algorithm is provided security from malicious insiders and threats during the processing of the data. Further, a relatively advanced attribute based encryption algorithm is proposed with collaborative access control, for public cloud storage. The proposed algorithm will be suitable for the application or the data that needs high level security. The accessed time is also reduced where which cost is reduced comparatively.

References

[1] Chaudhari N, Saini M, Kumar A and Priya G 2016 A Review on Attribute Based Encryption 8th Inte. Conf. on Comp. Inte. and Comm. Netw. Tehri, 380-385
[2] Kumar P P, Kumar P S and Alphonse P J A 2017 An Efficient Ciphertext Policy-Attribute Based Encryption for Big Data Access Control in Cloud Computing Nint. Inte. Conf. on Adva. Comp. Chennai 114-120
[3] Sethi K, Pradhan A, Punith R and Bera P 2019 A Scalable Attribute Based Encryption for Secure Data Storage and Access in Cloud Inte. Conf. on Cybe. Secu. and Prot. of Digi. Serv. (Cybe. Secu. ) Oxford United Kingdom 1-8
[4] Islam M, Shah M, Khan Z, Mahmood T and Khan M J 2015 A New Symmetric Key Encryption Algorithm Using Images as Secret Keys 13th Inte. Conf. on Fron. of Info. Tech. Islamabad 1-5
[5] Manjusha R and Ramachandran R Comparative study of attribute based encryption techniques in cloud computing Inte. Conf. on Embe. Syst. Coimbatore 116-120
[6] Tan S, Yeow K and Hwang S O 2019 Enhancement of a Lightweight Attribute-Based Encryption Scheme for the Internet of Things IEEE Inte. of Thin. Jour. 6 4 6384-6395
[7] Boneh D, Di Crescenzo G, Ostrovsky R, Persiano G, Cachin C and Camenisch J 2004 Public key encryption with keyword search in Adva. in Cryp. Berlin Germany:Springer-Verlag 3027 506-522
[8] Tang Q 2011 Towards public key encryption scheme supporting equality test with fine-grained authorization Proc. Aust. Conf. Inf. Secu. Priv. 6812 389-406
[9] Ma S, Huang Q, Zhang M and Yang B 2015 Efficient public key encryption with equality test supporting flexible authorization IEEE Tran. Inf. Fore. Secu. 10 3 458-470
[10] Sedghi S, Van Liesdonk P, Nikova S, Hartel P and Jonker W 2010 Searching keywords with wildcards on encrypted data in Secu. and Cryp. for Netw. Berlin Germany:Springer-Verlag 6280 138-153
[11] Bagath Basha C and Rajaprakash S 2019 Securing Twitter Data Using Phase I Methodology Inte. Jour. of Scie. & Tech. Rese. 1952 1955
[12] Bagath Basha C and Rajapraksh 2020 Enhancing The Security Using SRB18 Method of Embedding Computing Micr. and Micr103125.