Secure Data Retrieval based on Attribute-based Encryption in Cloud

Chaudhari Swapnil H.
P.G. Student
SSVPS's BS Deore College of Engineering,
Dhule, 424005,
India

Mandre B.R.
Associate Professor,
SSVPS's BS Deore College of Engineering,
Dhule, 424005,
India

ABSTRACT

Cloud computing plays important role in the development of IT industry. It can help a small organization to headway their business. An organization can progress from small scale industry to large scale industry. "Cloud" basically internet based data, network, resource storage. Meanwhile security, integrity, confidentiality requirement need must be achieve by cloud implementation. Attribute based encryption policy provides efficient encryption of data. Hierarchical implementation implies that an organization able to assign different privileges to users according to their role, using a top to bottom approach. Cloudsim has made virtual environment of cloud for developers. It connects to virtual resources according to user requirement of network resources. This paper describes the implementation of Hierarchical attribute base encryption scheme on cloudsim tool. Implementing attribute based encryption where rijndael algorithm used to encrypt data. Also paper include efficiency of encryption and decryption scheme used in implementation

Keywords

Encryption**,** Security, multiuser access**,** Ciphertext Policy Attribute based encryption **(**CP-ABE), Cloudsim, cloud computing, data sharing

1. INTRODUCTION

Cloud computing is one of important sourcing that enables organizations to move from traditional data storage and maintain within organization boundaries with cost effectiveness. Nowadays most of IT industry/ organization uses cloud infrastructure widely and provide shared access to network resources and data to users. Cloud implementation has proved rapid growth as it operates at fast speed and requires very less maintenance. The cloud service model provides services to users as per their requirement. So any Organization can select service as their need to meet its requirement. Virtualization of hardware and its availability reduces dependency and investment on required hardware. Cloud application programming interface (API) allows developers and users to access cloud services efficiently. Users can connect to cloud services through a web services using web browsers so access to cloud services are not dependent on a particular location and device. Sharing of data and require resources on cloud computing allows to increase user productivity by reducing system response time. As data security is an important aspect of the organization data sharing and deployment model of cloud computing can be effectively used to increase the complexity level of security.

Now days in market cloud computing provide different service oriented models have been available, models like 1) IaaS-Infrastructure as a Service, 2) PaaS-Platform as a Service, and 3) SaaS-Software as a Service. Many commercial cloud computing systems have been built at different levels, e.g., Amazon's S3 [3], Amazon's EC2 [2], and IBM's Blue Cloud [4] are IaaS systems, while Engine Yard[3], Google App Engine [5] and Yahoo Pig are representative PaaS systems, and Google's Apps [6] and Salesforce's Customer Relation Management (CRM) System [7] belong to SaaS systems. With these cloud computing services, the enterprise users no longer need to empower in hardware or software systems or hire professionals to maintain these systems, thus they save cost on IT infrastructure and human resources; and also different computing utilities provided by cloud computing are being provide at a comparatively low price in a pay-as-you-use manner[1].

In spite of the fact that the great benefits introduce by cloud computing paradigm are exciting for organization, academic researchers, and widely cloud users, security problems in cloud computing become serious barrier which, without considering, will put a stop to cloud computing large applications and usage in the future. One of the important security concerns is data privacy and data security in cloud computing because of its Internet-based data storage and management. In cloud computing, data users have to provide data to the cloud service provider for storage and various business operations, while the cloud service provider is usually a third party which cannot be totally trusted. Data is very important property for any organization, and users will face serious problems if its confidential data is reveal to their competitors or the public. Thus, cloud users initially want to make sure that their data are kept secret and confidential to the cloud provider and their potential competitors. This is the first data security requirement.

Access control is one of the classic security concept which came in focus in 1960s or early 1970s [9], and different access control models have been proposed since then. One of them, Bell-La Padula (BLP) [10] and BiBa [11] are two security models. To achieve flexible and fine-grained access control, a number of schemes [2],[12]–[15] have been proposed more recently. All these schemes are applicable where the data owner and the service provider must in same domain. Since every time data owner and service provider not in the same domain in cloud computing ,a new access control model come in focus attribute based encryption [16] it is proposed by Yu et al.[17], that model is called Key policy attribute based encryption(KP-ABE) KP-ABE supports fine grained access control. However, KP-ABE have some limitation it it falls in flexibility in attribute management and also lack in dealing with multi-level attribute authentication. Ciphertext- policy attribute based encryption (CP-ABE)[18] which support the KP-ABE limitations. In this system, a ciphertext-policy attribute based encryption (CP-ABE,) scheme by Bobba *et al.* [19] with a hierarchical structure of system users, where encryptions perform by Rijndael encryption algorithm.

Here in next sections of application area and its implementation in detail. The paper is organized as follows, section 2 background describes the literature survey for the implemented scheme, section 3 describes the related work with its features and characteristics, section 4 implementation details describe module information, section 5 describes the result of implementation, and section 6 consist of conclusion and future scope.

2. BACKGROUND

Data security challenges describe aspect like can data owner and user protect data from improperly accessed? Every data owner wants unauthorized user must not access his data. They don't want cloud provider to mine his data for their marketing purpose. So data need access control then only authorized parties can access data.

Access control technique provided by the cloud service provider is determining the access in to cloud environment. If access control technique is week it will lead to different attacks like collusion attacks, denial of service attack and insider attack. Every user need to get fine grained access control in cloud environment have an access control policy. There are so many access control policies available in market for cloud computing like Mandatory access control (MAC), Discretionary access control (DAC), Role based access control (RBAC) and Attribute based access control (ABE).

Public Key Infrastructure (PKI) is one which achieve trust in cloud computing. Several algorithms are basically based on PKI. The generic public key Infrastructure encryption and decryption process start with data sender or owner requesting public key form Key Distribution center (KDC). Then PKI assign the public key and sends to requester. Using that public key data will encrypted by the sender for receiver. Receiver use private key to decrypt data.

Attribute based encryption was initially introduced by Sahai and waters[3], it was new method which used fuzzy identity based encryption .In the ABE scheme, in with ciphertexts are never encrypted to any one particular user as like traditional public key cryptography. It prefers, both user decryption key and ciphertexts are associated with the attributes or a policy over that attributes. Only user is able to decrypt a ciphertext if there is a match between ciphertext and users decryption key. ABE schemes are classified into two schemes key-policy attribute based encryption (KP-ABE) and ciphertext-policy attribute based encryption (CP-ABE), depending how attributes and policy are associated with ciphertexts and users' decryption keys.

In a KP-ABE scheme [16], a ciphertext is correlated with a set of attributes and a user's decryption key is correlated with a tree access structure that tree access structure is monotonic access structure. Only if the attributes related with the ciphertext satisfy that monotonic tree access structure, can the only user decrypt the ciphertext. In a CP-ABE scheme [18], the working of ciphertexts and decryption keys are switched. In the CP-ABE ciphertext and tree access policy which is chosen by data Encryptor are encrypted together while the corresponding decryption key is created with respect to a attribute set.

As long as the attributes set associated with a decryption key that satisfies the tree access policy associated with a given ciphertext, the key can be used to decrypt the ciphertext. Since the users' decryption keys are related with a set of attributes, CP-ABE is conceptually closer to traditional access control models such as Role-Based Access Control (RBAC) [18]. Thus, used of CP-ABE are more practical used over KP-ABE for efficient use of access control of encrypted data. But CP-ABE scheme have limitation of flexibility issue [3].

Rakesh Bobba et al find the flexibility issue of CP- ABE and give the solution of attribute set recursive structure which is basically known as (CP-ASBE) [4]. Guojun Wang et al produce a scheme to provide fine grained access control by a combination of hierarchical identity-based encryption (HIBE) system and ciphertext-policy attribute-based encryption (CP-ABE) [5]. Zhiguo Wan et al started Hierarchical attributes-set-based encryption (HASBE) by extending the ASBE and CP-ABE with hierarchical implementation. They have provided the flexibility and scalability with their solution, but suffer from time overhead of encryption and decryption, complex key structure and problem in searching particular document [1].

3. RELATED WORK

This section consists of detail explanation of related work.

3.1 Hierarchical identity-based encryption

The identity-based encryption (IBE) system introduced by Boneh and Franklin, (2001), where every user get private key by the private key generator (PKG) who distribute private keys to each user that is in practical for large scale network because PKG has a overloaded by creating private key for each user and distribute it[8]. Gentry and Silverberg (2002), who find the solution to reducing the overhead of the root PKG, by introducing a scheme HIBE, Their scheme with collusion resistance at an arbitrary number of levels has select ciphertext security under the random oracle model and the Bilinear DiffieeHellman (BDH) assumption. A construction of Boneh and Boyen (2004) proposed a HIBE system along with selective-ID security under the BDH consideration without random oracles. In these constructions, the length of Private Key and ciphertext, as well as the time required to encryption and decryption grows linearly with the depth of the hierarchy. For better performance, Boneh et al. (2005) proposed an efficient HIBE system which used only a constant number of bilinear map operations during decryption and a constant length of ciphertext. Using identity-based broadcast encryption with key randomization Gentry and Halevi (2009) proposed a fully secure HIBE scheme, and using a dual system encryption Waters (2009) achieved full security in systems.

3.2 Attribute-based encryption

The notion attributes based encryption initially introduced by Sahai and waters in 2005[3]. Referring ABE Goyal et al. 2006 proposed a fine-grained access control attribute based encryption using monotonic access structure. That scheme is classifies as Key-policy attribute based encryption (KP-ABE) where the attribute are describe the ciphertext and access structure is specified in the private key. A succeeding construction by Ostrovsky et al. (2007) it allows for non-monotonic access structures. Bethencourt et al. (2007) work on a ciphertext-policy ABE (CP-ABE) scheme, in which the roles of the ciphertext and keys are switch in contrast with the KP-ABE scheme. Muller et al. (2008) introduced an efficient distributed attribute-based encryption (DABE) scheme which use disjunctive normal form (DNF) policy during the bilinear map operations to perform decryption. Both of the above mentioned CP-ABE schemes provide a security under the random oracle model and the generic bilinear group model [13]. (Wang et al.) Scheme is proposed for secure data sharing in cloud servers by using a conjunctive fuzzy and precise identity-based encryption (FPIBE). The FPIBE scheme is work efficiently to achieve a flexible access control, by partitioning the access control policy into two parts: an attribute-based access control policy and a recipient identity (ID) set. Using the FPIBE scheme, a data owner can encrypt data by specifying a recipient ID set, or an access control policy over attributes, so that only the user whose ID belonging to the ID set or attributes satisfying the access control policy can decrypt the corresponding data. Even so, it does not address the scalability issue. Yu et al. (2010b) combined KP-ABE, proxy re-encryption (PRE) (Blaze et al., 1998), and lazy to achieve a scalable revocation process in cloud computing [14]. However, the technique in Yu et al (Boneh et al., 2005) cannot be applied directly to combine PRE and CP-ABE Since in KP-ABE, access structure is basically associated with data other than the users attribute key. The Wang et al., (2010) and Yu et al.(2010a) is the first introduce combination of CP-ABE and PER technique. The limitations of the scheme are as follows: the CP-ABE scheme implemented only considering “AND” semantic in the access control and does not support key delegation, and the former lack of security proof for the encryption scheme and decryption for the revocation scheme.

3.3 Contribution

Basically in Cloud computing system consists of five types of parties: a *cloud service provider*, *data owners*, *data consumers*, *domain authorities*, and a *trusted authority*.

All services that provided by cloud managed by cloud service provider. Data owners initially encrypt their data files and store them in the cloud that store data share with data consumer. To access that shared data and, data consumer first need to download encrypted data files of their need from the cloud and then decrypt with same algorithm used to encrypt them. Each and Every data owner or data consumers are managed by a domain authority. Data owners, data consumers, domain authorities, and the trusted authority are organized in a hierarchical manner.

While implanting a system structure of an organization consider which consists of different departments like Account, Purchase, Sale and Quality. All departments are control by highest centralized authority. Every department has a departmental head called as “General Manager” and other employees working at a lowest level. This hierarchical structure consider for implementation. For the encryption and decryption processes Rijndael algorithm is being used.

4. IMPLEMENTATION DETAILS

In this section consist of implementation detail of a system.

4.1 Data Encryption and Decryption process

The system used rijndael algorithm to perform encryption and decryption of data. This works as follow

4.1.1 Encryption of Data

While performing encryption process consider some set of attribute values assigned to the user in the system.

Consider AVS = {a1, a2, a3…} is set of attribute values assigned to the system user.

1. Encryption algorithm takes every attribute value and data file as input.
    - Input: Attribute value and data file
2. Rijndael algorithm performs encryption on byte arrays. To perform encryption so string value of attribute and data file are converted into a byte.
    - getbytes() method convert String in to bytes.
3. Using rijndael algorithm key generated and encryption is performed

4.1.2 Decryption of Data

Consider these sets of encrypted attribute values EA= {ea1, ea2, ea3}

1. Decryption algorithm takes every encrypted attribute value and data file as input
    - Input: Encrypted attribute value and data value
2. Rijndael algorithm performs Decryption on byte arrays. So encrypted string value of the attribute is converted into a byte.
    - Convert ea1 into getbyte ()
3. While decryption of encrypted data users public key and private key are use and also policy is check if it matches decryption is performed.
4. Decrypted file is view to authorized user.

5. EXPERIMENTAL RESULTS

In this section resultant graph is shown.

5.1 Time Require for Encryption

In this graph time require for encryption by proposed system are shown. It shows that reduction in time and since using Rijndael algorithm encryption process is to strong.

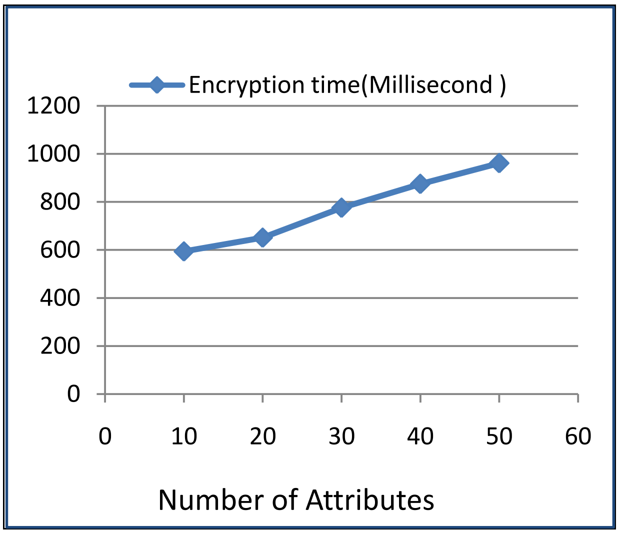

Figure 5.1 Time required by Rijndael in theProposed Hierarchical CP-ABE system

5.2 Time require for Decryption

In this graph time require for decryption by proposed system figure 5.2 where user’s private key which is generated on the based attribute assigned to user. So while decryption process no need to decrypt all attribute so it require less time than existing system.

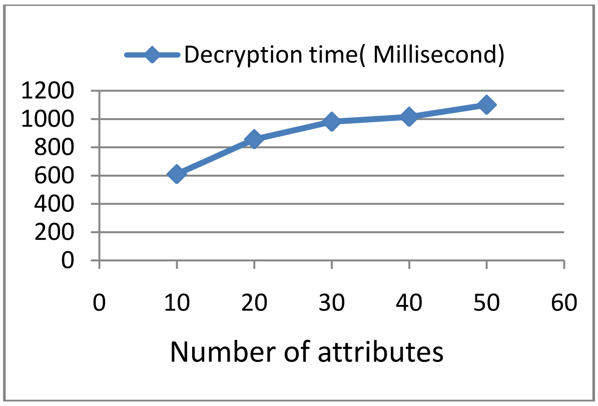

Figure 5.2 Time required to decrypt attributes by theProposed Hierarchical CP-ABE system

5.3 Key size

In CP-ABE Scheme private key assign to user which is computed using user's attribute. Which use each character of attributes is considered and generates a new value which is alphanumeric value. So it has overcome the limitation of exacting HASBE system of complex key size to remember.

5.3 .1 Encryption Key generation time

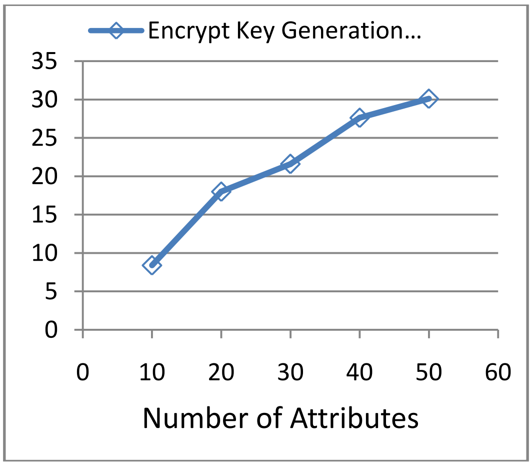

Figure 5.3 Time required to Generate Encryption Key for number of attributes by proposed system

5.3.2 Decryption Key generation time

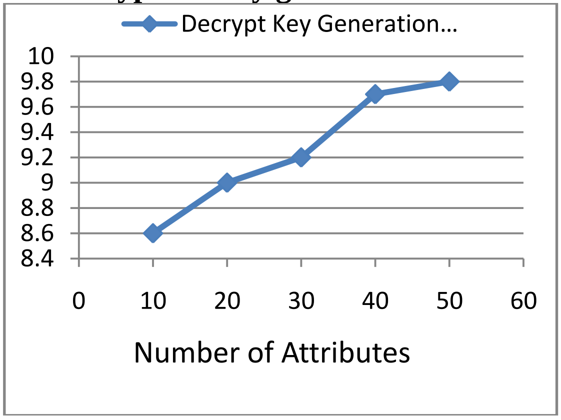

Figure 5.3 Time required to Generate Decryption Key fornumber of attributes by proposed system

6. CONCLUSION

This paper explains about the implementation of ciphertext policy attribute based scheme using Rijndael encryption decryption algorithm. Where consider Hierarchical CP-ABE scheme by addressed the issue of time require for encryption and decryption overhead and reduce generation of complex key. The Proposed work provides easy and simple to and understandable key structure. As future scope, multiple organizations and implement it on different cloud to scale up the business idea.

7. REFERENCES

[1] Zhiguo Wan, Jun'e Liu, and Robert H. Deng, "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing", *in IEEE Transactions on information* forensics and security, Vol. 7, No. 2, in April 2012.

[2] Schucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou," Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc IEEE INFOCOM,2010.

[3] A.Sahai and B.Waters,"Fuzzy Identity Based Encryption," In Proc. Advances in Cryptology-Eurocrypt,2005, vol.3494,pp.457-473.

[4] S.Muller, S.Katzenbeisser, and C.Eckert," Distributed attribute-based encryption,"in Proc.11th Int.Conf.Information Security and Cryptology, 2008,pp.20-36, Springer.

[5] J.Hur and Dong Kun Noh," Attribute-Based Control with Efficient Revocation in Data Outsourcing systems," IEEE Transactions on Parallel and Distributed Systems,Vol.22, No.7,July 2011.

[6] V.Goyal, O.Pandey, A.Sahai and B.Waters, "Attribute- based encryption for fine-grained acess control of encrypted data," in Proc.ACM Conf.Computer and Communications(ACM CCS), Alexandria,VA,2006.

[7] J.Bethencourt, A. Sahai, and B.Waters, "Ciphertext-policy attribute based encryption," in Proc.IEEE Symp. Security and Privacy, Oakland, CA,2007.

[8] R.Bobba, H.Khurana and M.Prabhakaran," Attribute-sets: A practically motivated enhanced to attribute-based encryption," in Proc.ESORICS, Saint Malo, France, 2009.

[9] G.Wang, Q.Liu, and J.Wu," Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in Proc.ACM Conf. Computer and Communication security(ACM CCS), Chicago.IL,2010.

[10] M.Cahse," Multi-authority attribute based encryption," inProc.TCC'07, 2007,pp.515-534, Springer.

[11] Yongdong Wu, Zhuo Wei, and Robert H.Deng,"Attribute- Based Access to Scalable Media in Cloud-Assisted Content Sharing Networks," IEEE TRANSACTION ON MULTIMEDIA,Vol.15, No.4, June 2013.

[12] Kan Yang, Xiaohua Jia, KuiRen,Bo Zhang,and Ruitao Xie,"DAC-MACS:Effective Data Access Control for Multiauthority Cloud Storage Systems," IEEE

Transaction on Information Forensics and Security, Vol.8,No.11,Nov 2013 .

[13] M.Green, S.Hohenberger, and B.Waters,"Outsourcing the decryption of ABE ciphertexts," in proc.USENIX Security Symp., San Francisco, CA,USA,2011.

[14] M.Green, S.Hohenberger, and B.Waters,"Outsourcing the decryption of ABE ciphertexts," in proc.USENIX Security Symp., San Francisco, CA,USA,2011.

[15] Rafail Ostrovsky, Amit Sahai, Brent Waters: Attribute- based encryption with non-monotonic access structures. ACM Conference on Computer and Communications Security 2007: 195-203.

[16] Dongyoung Koo, Junbeom Hur, Hyunsoo Yoon, Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage, Computers & Electrical Engineering, Volume 39, Issue 1, January 2013, Pages 34-46, ISSN 0045-7906.

[17] Shuaishuai Zhu; Xiaoyuan Yang; Xuguang Wu, "Secure Cloud File System with Attribute Based Encryption," *Intelligent Networking and Collaborative Systems (INCoS), 2013 5th International Conference on* , vol., no., pp.99,102, 9-11 Sept. 2013.

[18] Zhou Wei; Pierre, G.; Chi-Hung Chi, "CloudTPS: Scalable Transactions for Web Applications in the Cloud," *Services Computing, IEEE Transactions on* , vol.5, no.4, pp.525,539, Fourth Quarter 2012.

[19] Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters: Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. IACR Cryptology ePrint Archive 2006: 309 (2006).