International Journal of Research in Advent Technology, Vol.2, No.9, September 2014
E-ISSN: 2321-9637

An Assessment on Identity Based Encryption Mechanisms in Cloud Computing

Dr.V.VENKATESA KUMAR[1], M.NITHYA[2], Mr.M.NEWLIN RAJKUMAR[3],
Computer Science Engineering[1, 2, 3,]
Anna University Regional Centre,Coimbatore[1, 2, 3]
Email: Nithyamani1.1@Gmail.Com[2]

Abstract- Cloud computing is an emerging trend at present, in which cloud providers can remotely store the data in the cloud in a server and provide the services to the cloud user's on-demand via the internet. Data sharing is the major concern in cloud storage. Data Security and privacy are the critical issues for remote data storage. In order to share the data securely, it is necessary to adopt an efficient encryption system. Identity Based Encryption is a public key based encryption in which the public key of the user contains some distinct information about the user's identity (e.g. User's email address). In this paper, we are going to analyze various schemes that are used for encryption and possible solutions for their limitations, which consist of Identity Based Encryption (IBE), Biometric IBE, Fuzzy IBE and Identity Based Hash Proof System (IB-HPS).

Index Terms- Identity-based encryption; biometric; fuzzy; hash proof system.

1. INTRODUCTION

Cloud computing is a model in which the resources are shared by the cloud users via internet. Resources include servers, files, network, applications and services. The important features of cloud computing are

- A broad network access
- Resource pooling
- Rapid elasticity
- Measured service
- Multi-tenancy
- On-demand self service

A variety of applications are used in the cloud.some few applications are

(1) Mozy
(2) Skype
(3) Box
(4) QuickBooks
(5) Facebook
(6) Twitter

The main goal of cloud computing is the data sharing. While sharing the data, security is needed [1]. For security concept, cryptographic techniques are used. Cryptographic technique is used for protecting the data by converting original information into some other forms. To invoke such techniques, two types of encryption schemes are used. They are symmetric key and asymmetric key encryption. In symmetric key encryption, the same key is used for encryption. So, it is not secure. In asymmetric key encryption, for encryption and decryption [2] two different keys are used. In this paper, we are focusing new public key encryption called IBE and the various schemes of IBE.

2. LITERATURE SURVEY

The literature surveys that contain the study of different schemes available in Identity Based Encryption (IBE) that are Fuzzy IBE, Biometric IBE and IB-HPS.

2.1. *Identity-based encryption*

Identity-Based Encryption is a public key encryption of a user contains some distinct information about the user's identity. In IBE, one's publicly known identity is used as public key where the corresponding private key is generated by the trusted authority for the known identity. The trusted authority is also called Private Key Generator (PKG). IBE scheme is proposed to avoid the collision of a secret key pair. For example, if Alice wants to encrypt messages for Bob means she uses Bob's identity (e.g. Email address) as her public key and for decrypting the message, Bob uses his private key (e.g. Password) that is generated from PKG.

The following figure1 represents the schematic representation of IBE. Referring the diagram, data owner is also called cloud provider. Data owner is an organization that provides the services to the cloud users via the internet. Cloud users are also called cloud consumers. A cloud user uses the hosted service that has been produced by the data owner. The private key generator is also called trusted authority that will generate the distinct secret key id for both data owner and cloud user. Based on the secret key id, data owner will host the encrypted data in the cloud. Cloud user browses the hosted data that have been hosted by the cloud provider by using the distinct secret key id.

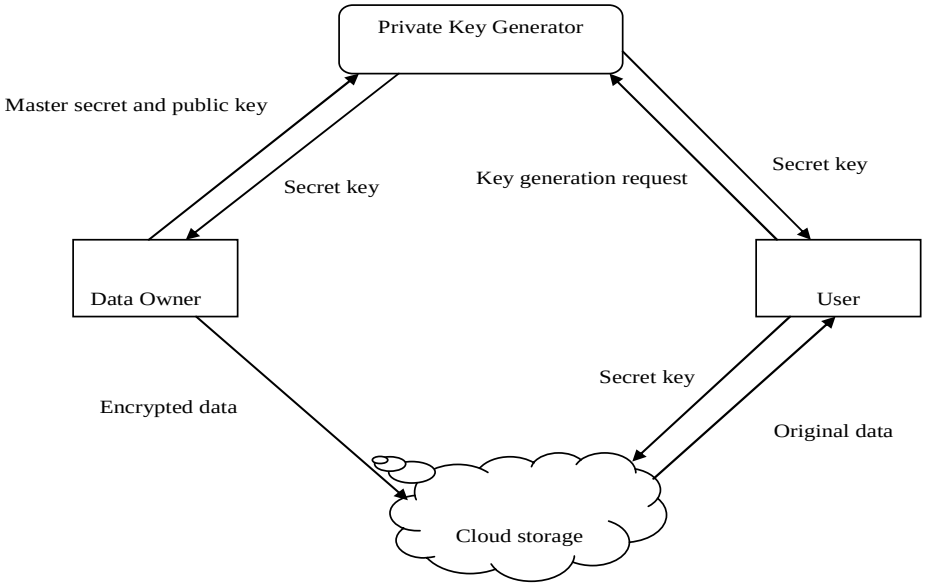

Fig. 1.Schematic representation for IBE

2.1.1. Algorithm for IBE

The IBE encryption scheme consists of the following four probabilistic polynomial time algorithms [3]:

(1) Setup

In the setup module, the public key and secret key parameters of data owners will be created.

(2) *Key Generation*

In the key generation algorithm, the secret identity key sk_{id} is generated for the decryption purpose. The secret identity key for the individual cipher text classes will be generated by using the corresponding cipher text class id and the master secret key msk.

(3) Encrypt

The encryption is done by using the corresponding cipher text class id I and the message M. After encryption the cipher text will be produced. The encryption is done as Encrypt (I, M).

(4) Decrypt

The decryption will be done by the authorized user to decrypt the corresponding cipher text class that he/she required. Decryption is done as follows: Decrypt (C, sk_{id}). Here C is the cipher text which is to be decrypted and sk_{id} is the secret identity key.

- The advantage of IBE scheme is that the private keys to the corresponding user are kept secure.
- The problem with IBE scheme is that the adversary could reset the password back to mailed one because the identities are not unique. User ID's can be easily changed.

2.2. ***Biometric Identity Based Encryption (Biometric IBE)***

The modified scheme of IBE is called Biometric IBE. Biometrics refers to the authentication techniques that include physiological and behavioral features of the individuals that can be automatically verified [6]. Examples of biometrics are fingerprints, hand geometry, iris scan, retina scan, signature, face and voice. Depending upon the context, there are two approaches to resolve a person's identity in the biometric system. They are verification and identification. In the verification process, a sample is compared against a stored template. In identification process, a sample search against the database of templates. The following table1 describes the list of comparisons for various types of biometrics. An application of biometrics includes PC access and internet security (laptop security, internet security), physical area security (voting, banking, prisons and military), mobile phones (network access and theft protection) and mobile finance transaction (credit cards and ATM cards**).**

It improves the disadvantage of IBE by Authenticating the biometrics of a person directly. Biometrics of a person cannot be shared or used by others. Biometric features are difficult to steal. Biometric systems provide a confidence in identifying the user identity. Biometric of a person is always available to the individuals so there is no need to remember such passwords or PINs.

The drawback of using biometric IBE is that biometric systems must not be able to accommodate changes over time due to some problems such as ageing or injury. In such cases, biometric devices are unavoidably noisy. So the accuracy of the biometric devices needs to be improved.

Table 1. Comparison of various biometric types

Biometric Types	**Examples**	**Description**	**Authenticity**	**Safety**
Physical biometrics	Fingerprint	Analyzing the fingertip patterns.	High	Medium
	Hand geometry	Measuring the shape of a hand.	Medium	High
	Iris scan	Analyzing the features of the colored ring of the eye.	Medium	Medium
	Retina scan	Analyzing blood vessels in the eye.	High	Low
Behavioral biometrics	Signature	Analyzing signature dynamics.	Medium	Medium
	Keystroke	Measuring the time spacing of the typed words.	Low	Medium

2.3. *Fuzzy Identity Based Encryption (Fuzzy IBE)*

Fuzzy Identity based Encryption is introduced in order to overcome the problems of Biometric IBE. Fuzzy IBE is a public key encryption in which a set of descriptive attributes is defined with a predefined error tolerance capability. In Fuzzy IBE, these attributes are used as used as one's known identity [5]. Error tolerance is defined as the identity that was used for encryption is not needed to be exactly the same as the one used for decryption. This encryption scheme uses the hamming distance as a metric in order to calculate the distance between two different identities and the distance between the two identities are always greater than the error tolerance factor [6].

2.3.1. Algorithm for fuzzy IBE

The fuzzy IBE encryption scheme consists of the following four algorithms [6]:

(1) Setup

Setup algorithm generates a master key for Alice for the given error tolerance factor d.

(2) Key Generation

In the key generation algorithm, Alice's identity w is being detected and generates Alice's private key for the given identity w.

(3) Encrypt

In encryption algorithm, Charlie can encrypt messages M with Bob's identity w'. After encryption the cipher text will be produced. The encryption is done as Encrypt (w', M).

(4) Decrypt

In this algorithm, Bob can decrypt messages M with his private key. Alice can also decrypt message M with her private key with $|w \cap w'| >= d$.

2.3.1.1 Advantage and Disadvantage of fuzzy IBE

- The advantage of the Fuzzy IBE scheme is that Alice can decrypt messages with her private key encrypted with her own identity w. Alice can also decrypt messages encrypted with other identity w' if $|w \cap w'| >= d$.

- The problem with the Fuzzy IBE scheme is that the adversary can easily guess the identity and attributes means messages can be easily decrypted. By doing this, information is easily leaked.

2.4. *Identity Based Hash Proof System (IB-HPS):*

Another modified form of IBE is called IB-HPS. IB-HPS is a kind of public key encryption in which the message will be encrypted by using the cipher text id which will be encapsulated with the encapsulation key before transferring and the receiver will decrypt the message by using identity secret key, if the received cipher text is encapsulated with the encapsulated key [4] [8]. In IB-HPS, Master's public key and secret key will be produced by using the secret parameter. The Master public key will consists of an Encapsulation key set and cipher text identifier set. Initially the identifier secret key will be generated by using the master secret key and the cipher text id. The invalid encapsulation is done after valid encapsulation where the duplicate cipher text is encrypted with original cipher text id. In this method, leakage is prevented based on the Diffie-Hellman bilinear assumption [3] [7]. The following table2 describes the various symbols that are used in our IBE encryption Schemes.

Table 2: The various symbols used in IBE encryption schemes

Symbol	**Meaning**
mpk	Master public key
msk	Master secret key
sk_{id}	Secret identity key
I	Cipher text class id
M	Message
C	Cipher text
w, w′,w″	Fuzzy identities
d	Error tolerance factor

3. CONCLUSION

In this paper, we analyze different Identity based encryption schemes: Identity Based Encryption (IBE), Biometric IBE, Fuzzy IBE and IB-HPS. Among these schemes, IB-HPS scheme provides the better leakage resilient concern.

REFERENCES

[1] Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren and Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage",IEEE TRANSACTIONS ON COMPUTERS, FEBRUARY 2013.

[2]Cheng-Kang Chu, Sherman S.M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng, "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage",IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS", FEBRUARY 2014.

[3] Sherman S.M. Chow, Yevgeniy Dodis, Yannis Rouselakis, "Practical Leakage-Resilient Identity-Based Encryption from Simple Assumptions".

[4] Moni Naor, Gil Segev, "Public-Key Cryptosystems Resilient to Key Leakage".

[5] Amit Sahai and Brent Waters,"Fuzzy Identity-Based Encryption," January 31, 2010.

[6] Emmanuel Tsukerman, "Biometrics and Fuzzy Identity-Based Encryption".

[7] M. Choudary Gorantla, Raju Gangishetti and Ashutosh Saxena,"A Survey on ID-Based Cryptographic Primitives".

[8] Yu Chen, Zongyang Zhang, Dongdai Lin, Zhenfu Cao,"Generalized (Identity-Based) Hash Proof System and Its Applications".