International Journal of MC Square Scientific Research Vol.9, No.1 April 2017

SECURE AND EFFICIENT DATA CONTRIBUTION USING EXTENDED IDENTITY BASED ENCRYPTION IN CLOUD COMPUTING

K.Prabakaran
Department of Computer Science and Engineering, SRM University, Chennai, India
Email: prabakarankasivas@gmail.com

M.Prabu
Assistant Professor, Department of Computer Science and Engineering, SRM University, Chennai, India.
Email: manavalanprabu@gmail.com

Abstract— Cloud computing is used to share computing resources and data over internet. When sensitive data is shared over Internet, it should be transferred in secured manner. Data security is ensured using Identity Based Encryption mechanism. In the existing Cloud Computing system which is implemented using Identity Based Encryption mechanism, authorized user can share their credential to unauthorized user and data can be accessed by unauthorized user who hasn't subscribed to Cloud Computing System. To overcome this issue, we propose a notion called Extended Identity Based Encryption(E-IBE) system, which ensures authentication and confidentiality. In this approach, we use Kerberos authentication protocol along with Identity Based Encryption methodology to ensure authentication and confidentiality.

Keywords— Cloud Computing; Extended Identity Based Encryption;

1. INTRODUCTION

1.1 Context, literature review, rationale, structure

Cloud computing is a paradigm that provides massive computation capacity and huge memory space at a low cost [1]. It enables users to get intended services irrespective of time and location across multiple platforms (e.g., mobile devices, personal computers), and thus brings great convenience to cloud users. Among numerous services provided by cloud computing, cloud storage service, such as Apple's iCloud [1], Microsoft's Azure [3] and Amazon's S3 [4], can offer a more flexible and easy way to share data over the Internet, which provides various benefits for our society [5]. However, it also suffers from several security threats, which are the primary concerns of cloud users [6].

Using Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance[7]. Identity-based public key encryption facilitates easy introduction of public key cryptography by allowing an entity's public key to be derived from an arbitrary identification value, such as name or email address[8].

Original motivation for identity-based encryption was to simplify certificate management in e-mail systems. When Alice sends mail to Bob at bob@hotmail.com she simply encrypts her message using the public key string "bob@hotmail.com". There is no need for Alice to obtain Bob's public key certificate. When Bob receives the encrypted mail he contacts a third party, which we call the Private Key Generator (PKG). Bob authenticates himself to the PKG in the same way he would authenticate himself to a CA and obtains his private key from the PKG. Bob can then read his e-mail[9].

Identity-Based Encryption (IBE) which simplifies the public key and certificate management at Public Key Infrastructure (PKI) is an important alternative to public key encryption. However, one of the main efficiency drawbacks of IBE is the overhead computation at Private Key Generator (PKG) during user revocation[10].

Identity-based encryption is a promising cryptographical primitive to build a practical data sharing system. However, access control is not static. That is, when some user's authorization is expired, there should be a mechanism that can remove him/her from the system. Consequently, the revoked user cannot access both the previously and subsequently shared data[11]. Revocation is achieved by instructing the mediator to stop helping the user to sign or decrypt messages[12].

In Identity-based threshold signature (IBTHS) scheme, the round-complexity of the threshold signing protocol is optimal since each party pays no other communication cost except broadcasting one single message. The computational complexity of the threshold signing procedure is considerably low since there appears no other time-consuming pairing except two pairings for verifying each signature shares. It is the private key associated with an identity rather than a private key of the private key generator (PKG) that is shared among signature generation servers[13].

2. Basis For Extended Identity Based Encryption

Identity-Based Encryption (IBE) is an asymmetric cryptography technique. In this technique we use a public key to encrypt data and a private key to decrypt data. Identity of the user (e.g. Email address, PAN Number, Voter ID) is used as a public key. Data is encrypted using public key and ciphertext is generated. To decrypt ciphertext user needs to get a private key from a central authority called as Private Key Generator (PKG). In Cloud Computing, Identity-based Encryption technique is used to share data in secured manner.
Identity-based access control applied on the shared data should meet the following security goals:

2.1 Data confidentiality

Unauthorized users should not be allowed from accessing the plaintext of the shared data stored in the cloud server.

2.2 Backward secrecy

When a user's authorization is expired, or a user's secret key is compromised, he/she should not be allowed from accessing the plaintext of the subsequently shared data that are still encrypted under his/her identity.

2.3 Forward secrecy

When a user's authority is expired, or a user's secret key is compromised, he/she should not be allowed from accessing the plaintext of the shared data that can be previously accessed by him/her.

3. PROPOSED SYSTEM

In the existing Cloud Computing system which is implemented using Identity Based Encryption mechanism, one user can share their credential to another user and data can be accessed by another user(unauthorized user). To overcome this issue, we propose a notion called Extended Identity Based Encryption, which can provide the authentication and confidentiality. In this approach, we use Kerberos authentication protocol along with Identity Based Encryption to ensure authentication and confidentiality.

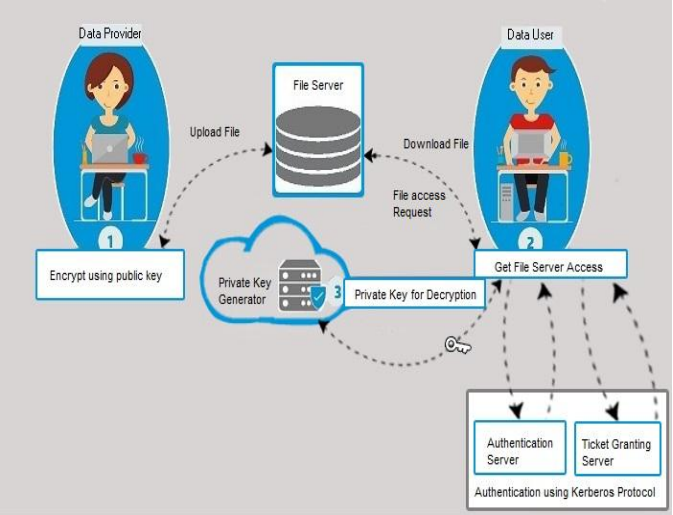

Figure 1: Extended Identity Based Encryption Architecture

3.1 Extended Identity Based Encryption Process

Step 1: The Data provider identifies the users(eg:Bob) who can access data from Cloud Server. Then, Data Provider encrypts the data using Identity(eg:Email ID) of user, and uploads the ciphertext of the shared data to the cloud server.

Step 2: User logs on to their system and send request to Authentication Server(AS) for authentication.

Step 3: Authentication Server(AS) verifies users privilege in its database, creates ticket-granting ticket and session key. Results are encrypted using a key derived from user's password.

Step 3: Once user receives response from Authentication Server(AS), they use password to decrypt received message, then sends ticket and authenticator that contain user name, network address and time to Ticket Granting Server(TGS) for getting service ticket.

Step 4: Ticket Granting Server(TGS) decrypts ticket and authenticator, verifies request, then creates service ticket for requested Cloud Server.

Step 5: User sends service ticket and authenticator to Cloud Server.

Step 6: Server verifies that ticket and authenticator match, then grants access to service.

Step 7: User download data in ciphertext format and decrypt it using Private Key received from Private Key Generator.

3.2 Kerberos Authentication

Kerberos is a network authentication protocol that works on the basis of token to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. It is mainly used in client–server model and it provides mutual authentication—both the user and the server verify each other's identity. Kerberos protocol uses strong cryptography so that clients can prove their identity to a server across an insecure network connection. Kerberos authentication protocol messages are protected against eavesdropping and replay attacks since messages are encrypted before transferring through network.

Kerberos has following components,

3.3 Authentication Server(AS)

Authentication Server checks if the user/client has authentication by searching the user name and password in the database. It offers a Ticket Granting Ticket that the user can send to the TGS to get a service ticket.

3.4 Ticket Granting Server(TGS)

A ticket granting server (TGS) is a component that is used by the Kerberos protocol as a trusted third party. A TGS validates request for network service access and provides a ticket for accessing service from server. The client who requires the service from the cloud service provider sends a service granting ticket request to the TGS using the ticket obtained from the authentication server. Service ticket is granted to client once request is validated.

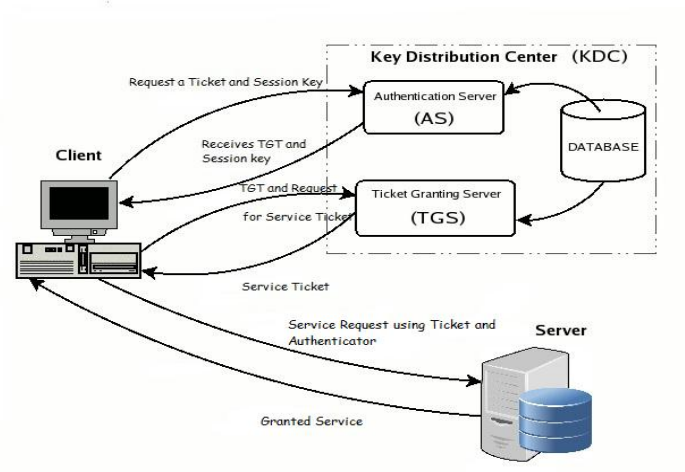

Figure 2: Kerberos Authentication Process

The processes to be performed by Kerberos are as follows.

Step 1: User logs on to their system and send requests to Authentication Server.

Step 2: Authentication Server verifies users access right in its database, creates a Ticket Granting Ticket and a session key. Results are encrypted using key generated from user's password and sent results to user.

Step 3: User decrypts incoming message using their password, then sends ticket and authenticator that contain client's name, network address and time to Ticket Granting Server.

Step 4: Ticket Granting Server decrypts ticket and authenticator, verifies request, then creates ticket for requested server.

Step 5: User sends ticket and authenticator to server.

Step 6: Server verifies that ticket and authenticator match, then grants access to service.

4. IMPLEMENTATION DETAILS

There are five modules in our proposed system.

1. Registration Module
2. Key Generation Module
3. File Uploading Module
4. Document Retrieval Module
5. Authentication Module

4.1 Registration Module

This module allows user to register to Cloud Service by entering information like name, email id, password, date of birth.

4.2 Key Generation Module

In this module, private key is generated for each user. User can decrypt the cipher texts using their private key and obtain the original files.

4.3 File Uploading Module

Files are encrypted using public key by data provider prior to outsourcing them to Cloud Servers.

4.3 Document Retrieval Module

The Cloud Server transfers the intended cipher text to data user after verifying their access permission. Data user can decrypt the cipher text by his secret key and obtains the original file.

4.4 Authentication Module

An authentication module gets user information such as user ID and password, and compares this information against entries in a database. If a user provides information that meets the authentication criteria, the user is validated and granted access to the requested resource. If the user provides information that does not meet the authentication criteria, the user is not validated and denied access to the requested resource.

5. CONCLUSION AND FUTURE WORK

Extended Identity Based Encryption system on Cloud Computing offers a high degree of security. In this paper an authentication framework, considering the security issues over the network during authentication process is proposed. The proposed protocol framework not only satisfies the need of authentication that is generally required in the protocol, it also provides the better security. This method would avoid any intrusion like phishing. This system can be evolved using Biometric-Kerberos based Authentication Protocol to provide further more security in Cloud Computing.

6. REFERENCES

[1]. L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner. "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review,vol 39.(2008).

[2]. iCloud. (2014) Apple storage service. [Online]. Available:https://www.icloud.com/

[3]. Azure. (2014) Azure storage service. [Online]. Available:http://www.windowsazure.com/

[4]. Amazon. (2014) Amazon simple storage service (amazon s3). [Online]. Available: http://aws.amazon.com/s3/

[5]. K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana. "Social cloud computing: A vision for socially motivated resource sharing," Services Computing, IEEE Transactions on, vol. 5, no. 4.(2012).

[6]. G. Anthes. "Security in the cloud," Communications of the ACM, vol. 53(2010).

[7]. C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou. "Privacy preserving public auditing for secure cloud storage". (2013).

[8]. DING, Xuhua and Tsudik, and Gene. "Simple Identity-Based Encryption with Mediated RSA".(2003).

[9]. D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," SIAM Journal on Computing, vol. 32.(2003).

[10]. Jin Li, Jingwei Li, Xiaofeng Chen, Chunfu Jia and Wenjing Lou. "Identity-based Encryption with Outsourced Revocation in Cloud Computing".(2015).

[11]. Jianghong Wei, Wenfen Liu, Xuexian Hu. "Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption".(2016).

[12]. D. Boneh, X. Ding, G. Tsudik, and M. Wong. "Efficient revocation and threshold pairing based cryptosystems".(2003).

[13]. Fei Li,Wei Gao,Guilin Wang,Kefei Chen and Xueli Wang. "Efficient identity-based threshold signature scheme from bilinear pairings in standard model". (2014).

[14]. D. Boneh, X. Ding, G. Tsudik, and M. Wong. "A Method for Fast Revocation of Public Key Certificates and Security Capabilities".(2001)

[15]. K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana."Social cloud computing: A vision for socially motivated resource sharing.(2012).

[16]. K. Yang and X. Jia. "An efficient and secure dynamic auditing protocol for data storage in cloud computing". (2013).