INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 4)
Available online at: www.ijariit.com

Storage identity based encryption in cloud for secure data sharing

M. Sandeep
sandeepmpersonnel@gmail.com
Saveetha School of Engineering, Kuthambakkam, Tamil Nadu

J. Mohana
mohanajaishankar1@gmail.com
Saveetha School of Engineering, Kuthambakkam, Tamil Nadu

ABSTRACT

Identity based public key system (IDPKS) is an attractive alternative to public key cryptography. ID-PKS setting eliminates the demands of public key infrastructure (PKI) and certificate administration in conventional public key settings. Due to the absence of PKI, the revocation problem is a critical issue in IBE settings. Several IBE schemes have been proposed regarding this issue in IBE settings. ID-based encryption (IBE) allows a sender to encrypt message directly by using a receiver's ID without checking the validation of public key certificate. Accordingly, the receiver uses the private key associated with his/her ID to encrypt such ciphertext. Since a public key setting has to provide a user revocation mechanism, the research issue on how to revoke misbehaving/compromised users. We propose a new IBE scheme with a cloud revocation authority (CRA) to solve the two shortcomings, namely the performance is significantly improved and the CRA holds only a system secret for all the users. Finally, we extend the proposed IBE scheme to present a CRA-aided authentication scheme with no period-limited privileges for managing a large number of various cloud services.

Keywords: *ID-PKS, Cryptography, CRA, Ciphertext, Encryption*

1. INTRODUCTION

Cloud computing is a type of Internet-based computing. Most of the time data will be shared using cloud computing. Cloud is a big area to access any type of data and information. It plays a major role in order to transfer the data safely and securely. Cloud provides a mechanism for shared computer processing resources. To provide extra security for data sharing in cloud computing is one of the big challenges. Sharing of data files between one and the other is a typical process in cloud computing as the data may contain some valuable information which has to been known only between the sender and the receiver. In this paper, a new Encryption technique has been introduced for sharing secure data between the sender and the receiver. The encryption and decryption technique provides more security in order to transfer data or files. So, in order to make the data transfer safely and securely between one and the identity-based encryption may be used for secure data sharing in cloud computing. The Identity Based Encryption technique provides both the forward and backward security which was absent in the previous techniques that were implemented. In this technique, the user may be able to access his/her data which have been transferred without any time limits. With authentication and authorization, the user may able to save or transfer the files from one user to another.

2. CRYPTOGRAPHY

Cryptography is a practice and study of a technique for secure communication in the presence of third parties called the adversaries. Cryptography prior to the modern age will be an effective synonymous with the help of a technique called the encryption and decryption. Cryptography is mainly used to transfer the data without allowing the third party users to access it so that the data can be intended for the users who have access to it.

Cryptography has been divided into two types and they are as follows:

- Symmetric Key Cryptography
- Public key Cryptography

2.1 Symmetric key cryptography: symmetric key cryptography refers to an encryption method in which both the sender and the receiver shares the same key. In symmetric key cryptography, a single key will be used by both the sender and the receiver for the encryption and decryption technique.

2.2 Public key cryptography: In Public key cryptography, a message can be encrypted by using the recipient public key, but it cannot be decrypted by anyone who does have the proper matching private key. This attempt is used to ensure proper security or confidentially.

3. ENCRYPTION AND DECRYPTION

For the process of transferring data safely and securely, the method of encryption and decryption have been proposed in this paper. In Encryption technique, the intended message or to be transferred or sent will be converted into some other formats (i.e., alphanumerical letters or numbers) which could be

understood only to the recipients who need to access the information or message. In Decryption technique, the intended file or the message sent by the recipient to the receiver will be converted into the original format which allows to user to access or read the information or the message received.

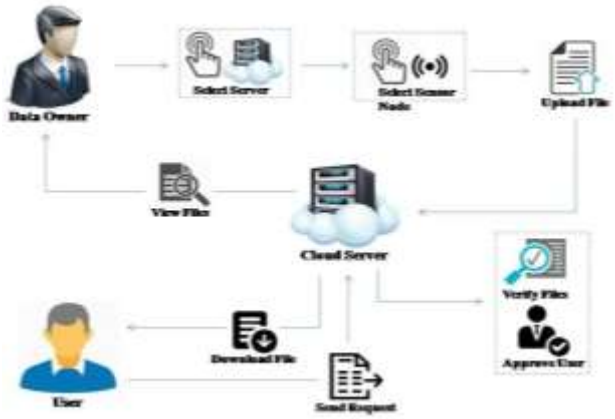

Fig. 1: Storage identity-based encryption

4. EXISTING SYSTEM

In the existing system, the immediate revocation method employs a designated semi-trusted and online authority (i.e., mediator) to mitigate the management load of the PKG and assist users to decrypt the ciphertext. In such a case, the online mediator must hold shares of all the user's private keys. Since the decryption operation must involve both parties, neither the user nor the online mediator can cheat one another. When a user is revoked, the online mediator can cheat one another. However, the online mediator must help users to decrypt each ciphertext so that it becomes a bottleneck for such schemes as the number of users grows enormously. All the users must periodically update new private keys sent by the PKG. As the number of users increases the load of key updates becomes a bottleneck for the PKG.

The disadvantages which have been found the existing system are:

- The Existing has less security.
- The updating of key fail enormously.

The Existing system has more un-scalability and inefficiency.

5. PROPOSED SYSTEM

In order to solve both the un-scalability and the inefficiency, a new Identity Based Encryption with cloud revocation authority have been proposed. A cloud revocation authority has been introduced to the scheme in order to hold a random secret value for all the users without affecting the security of the Identity Based Encryption scheme. The Cloud Revocation Authority (CRA) uses the master time key to generate the current time update key periodically for each non-revoked user and sends it to the user via a public channel. It is evident that our scheme solves the un-scalability problem of the KU-CSP. As the adversary model consists of two adversaries namely the inside adversary (or the revoked user) and the outside adversary. Finally, based on the proposed IBE scheme with CRA, a Cloud Revocation Authority aided authentication scheme with period-limited privileges for managing a large number of various cloud server

The Advantages of the proposed system are:

- The proposed has high security when compared to the existing system.
- The key operation has been a success.
- The inefficiency and the un-scalability have been reduced.

6. RESULT AND ANALYSIS

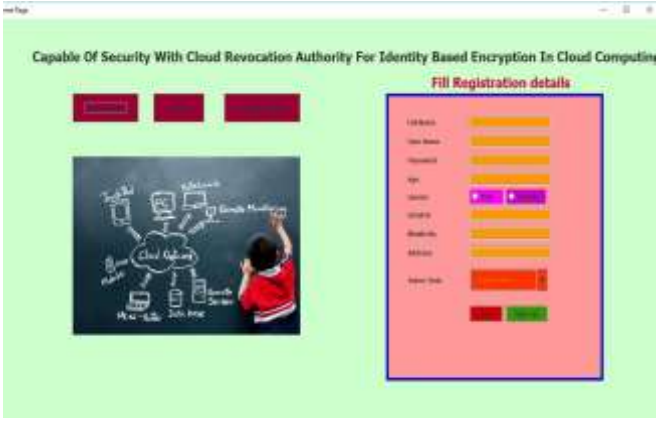

Fig. 2: Registration form

Shows the figure of Registration Form where the details of the Data Owner and the user needs to be filled.

Fig. 3: User Log in Page

Shows the figure of User Log in Page where the User needs to Log in for data sharing.

Fig. 4: Server log in Page

Shows the figure of Server Login Page in which the server has to be selected for the process of data sharing.

Fig. 5: File Verification Page

Shows the figure of File Verification Page in which the file will be verified and sent to the cloud storage.

Fig. 6: User Approval Form

Shows the figure of file approval page where the data Sent by the user will be approved by the cloud server.

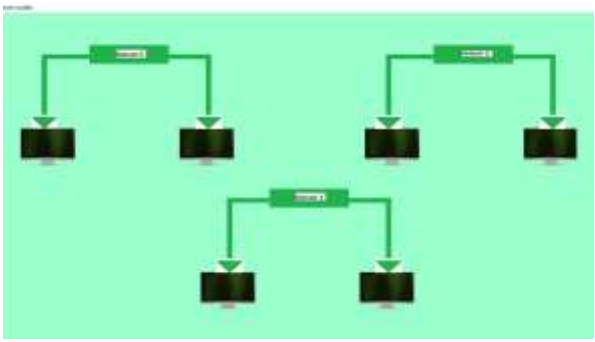

Fig. 7: Data sharing page and file download page

Shows the figure which appears after the successful file/data approved by the cloud server the data will be shared and downloaded

7. CONCLUSION

Cloud file sharing also was known as the cloud-based file sharing or online file sharing is a system in which user is allocated storage space on a file server which carries read and writes options on the file server. This proposed system will increase the security by introducing the identity-based encryption and decryption process which have been introduced in order to transfer the file from one user and the other within the cloud server. In this paper, we propose a scheme called storage identity-based encryption (SIBE) in order to build a cost-effective and secure data sharing in cloud computing which supports identity revocation and ciphertext update simultaneously such that the revoked user is prevented from accessing or sharing the file in the server.

8. REFERENCES

[1] Security Enhancement in Cloud using Identity-Based Encryption(IBE), IJARCCE International Journal of Advanced Research in Computer and communication Engineering ICRITCSA M S Ramaiah Institute of Technology, Bangalore Vol. 5, Special Issue 2, October 2016.

[2] Secure Data Sharing in Cloud Computing Using Revocable -Storage Identity-Based Encryption Jianghong Wei, Wenfen Liu, Xuexian Hu IJSDR1706010 International Journal Of Scientific Development and Research(IJSDR)

[3] Advance Secure Data Sharing in Cloud computing using Revocable Storage Identity-Based Encryption, International Journal for Research in Emerging Science and Technology, VOLUME-4, ISSUE-4, APR-2017 E-ISSN: 2349-7610.

[4] Survey: Identity-Based Encryption in Cloud Computing, International Journal of Science and Research(IJSR) ISSN(Online):2319-7064 Index Copernicus Value (2013) :6.14|Impact Factor(2014): 5.611

[5] Identity Based Encryption and Data Self Destruction in Cloud Computing International Journal on Recent and Innovation Trend in computing and Communication, volume 4 Issue: 7 ISSN: 2321-8169156-60.

[6] Authentic Data Sharing by Using Revocable-Storage Identity Based Encryption in Cloud Computing International Journal of Cloud computing International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) vol.4 special. issue 24 August. 2017.

[7] Data sharing in cloud computing using (RS-IBE) Revocable Storage Identity based encryption method IJARIIE-ISSN (O)-2395-4396 vol-2 Issue-5, 2017.

[8] Secure data sharing in cloud computing using Revocable Storage identity-based encryption. IEEE Transactions cloud computing (Volume:4, Issue 99 March 2016)

[9] Securing Cloud Services Using Revocable Identity Based Encryption JETIR (ISSN-2349-5162) March 2017, Volume 4, Issue 03.

[10] A secure data self-destructing scheme in cloud computing, IEEE TRANSACTIONS ON CLOUD COMPUTING VOL: PP NO:99 the YEAR 2014

[11] Data sharing in cloud computing using (RS-IBE) Revocable Storage Identity Based Encryption Method. Vol-2 Issue-52017 IJARIIE-ISSN (0)-2395-4396.

