IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 2, Apr-May, 2014
ISSN: 2320 – 8791 (Impact Factor: 1.479)
www.ijreat.org

Asymmetric Key Encryption with Privacy Preserving in Clouds

S. Ajitha[1], P.S. Apirajitha[2]

[1]PG Scholar, Department of Computer Science and Engineering, Sree Sastha Institute of Engineering and Technology, Chennai, India

[2]Assistant Professor, Department of Computer Science and Engineering, Sree Sastha Institute of Engineering and Technology, Chennai, India

Abstract

In this project, a new decentralized access control scheme for secure data storage in clouds is proposed , that support anonymous authentication. In this scheme the cloud verifies the authenticity of the server without knowing the user's identity before storing data. This scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The added feature of this project is access control, in which only valid users are able to decrypt the stored information. This project prevents replay attacks and supports creation, modification and reading data stored in cloud. In this scheme asymmetric key concept is used for encryption and decryption, so the security is high compared to the other project. Here the attributes and access policy of the users are hidden, so the security is high. In this project authentication scheme is collusion secure and protects privacy of the user. Moreover our authentication and access control scheme is decentralized and robust.

Keywords: *Access control, Authentication, Attribute-based signatures, Attribute-based encryption, Cloud storage, Replay attack, Anonymous Authentication.*

1. Introduction

The mainstay of this is to propose a new decentralized access control scheme for secure data storage in clouds that supports anonymous authentication.Clouds can provide several types of services like applications(e.g., Google Apps, Microsoft online),infrastructures (e.g., Amazon's EC2, Eucalyptus,Nimbus), and platforms to help developers write applications (e.g., Amazon's S3, Windows Azure). Many of the data stored in clouds is highly sensitive, for example , medical records and industry secrete information.

Security and privacy are thus very important issues in cloud computing. In one hand, the user should authenticate itself before initiating any transaction, and on the other hand, it must be ensured that the cloud does not tamper with the data that is outsourced. User privacy is also required so that the cloud or other users do not know the identity of the user. A cloud is called a public cloud when the cloud or other users do not know the identity of the user. A cloud is called a public cloud when the services are rendered over a network that is open for public use.Efficient searching operation on encrypted data is also an important concern in clouds. Here the clouds should not know the query but should be able to return the records that satisfy the query.This is perform by means of searchable encryption [9], [4].

Private cloud is cloud infrastructure operated solely for a single organization, whether managed internally or by a third-party and hosted internally or externally. Authentication of user using public key cryptographic techniques has been discussed in[10]. And also many homomorphic encryption techniques have been discussed [3], [15] to ensure that the cloud is not able to read the data while performing computations on them.Using the homomorphic encryption, the cloud receives ciphertext of the data and performing computations on the ciphertext and returns the encoded value of the result. And also in this project asymmetric key concept is used for encryption and decryption.

And also recently, Wang et al. [18] addressed secure and dependable cloud storage. Cloud servers prone to

Byzantine failure, where a storage server can fail in arbitrary ways[18]. The cloud is also prone to data modification and server colluding attacks. In this [18] paper explain the data encryption technique to store the data in cloud.so the security is high compared to the other schemes.

Cloud computing offers many benefits, but is vulnerable to threats. As cloud computing uses increase, it is likely that more criminals find new ways to exploit system vulnerabilities. Many underlying challenges and risks in cloud computing increase the threat of data compromise . To mitigate the threat, cloud computing stakeholders should invest heavily in risk assessment to ensure that the system encrypts to protect data, establishes trusted foundation to secure the platform and infrastructure, and builds higher assurance into auditing to strengthen compliance. Security concerns must be addressed to maintain trust in cloud computing technology.

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks, authentication is commonly done through the use of logon passwords. Knowledge of the password is assumed to guarantee that the user is authentic.

Access Control is any mechanism by which a system grants or revokes the right to access some data, or perform some action. Normally, a user must first Login to a system , using some Authentication system. Next, the Access Control mechanism controls what operations the user may or may not make by comparing the User ID to an Access Control database. Access Control system include: File permissions, such as create, read, edit or delete on a file server. Program permissions, such as the right to execute a program on an application server.Data rights, such as the right to retrieve or update information in a database.

Access control has three types they are User Based Access Control(UBAC), Role Based Access Control (RBAC), and Attribute Based Access Control (ABAC). ABAC is defined as, in which users are given attributes, and the data has attached access policy. Only users with valid set of attributes, satisfying the access policy, can access the data.The pros and cons of RBAC and ABAC are discussed in [6*].By means of ABE(Attribute Based Encryption), the records are encrypted under some access policy and stored in the cloud. Users are given sets of attributes and corresponding keys.Only when the users have matching set of attributes, can they decrypt the information stored in the cloud. In this paper [1] anonymous authentication is presented. For example, a user would like to store some sensitive information but does not want to be recognized. The user might want to post a comment on an article, but does not want his/her identity to be disclosed.ABS(Attribute Based Signature) is proposed by Maji et al. [11]. Here users have a claim predicate associate with a message. Claim predicate helps to identify the user as an authorized one, without revealing its identity. ABS and ABE both are combined to achieve authenticated access control without disclosing the identity of the user to the cloud.

Existing work [16], [8], [19], [17], [19], [14] on access control in cloud are centralized in nature.Except [16], and all other schemes in [16] uses a symmetric key approach and does not support authentication .And also some schemes [8], [14] do not support authentication. The existing system has one limitation that is the cloud knows the access policy for each record stored in the cloud. Existing work on access control in cloud are centralized in nature. Some scheme uses a symmetric key approach and does not support authentication. Some do not support authentication as well. Earlier work by Zhao *et al.* provides privacy preserving authenticated access control in cloud.

However, the authors take a centralized approach where a single key distribution center (KDC) distributes secret keys and attributes to all users. Unfortunately, a single KDC is not only a single point of failure but difficult to maintain because of the large number of users that are supported in a cloud environment., therefore, emphasize that clouds should take a decentralized approach while distributing secret keys and attributes to users. It is also quite natural for clouds to have many KDCs in different locations in the world. In this paper we use attribute based signature scheme [11] to achieve authenticity and privacy. Unlike [11], our scheme is resistant to replay attacks. And also our scheme allows writing multiple times which was not permitted in our earlier work [14].

2. Related Work

A new decentralized access control scheme for secure data storage in clouds that supports anonymous authentication is proposed. In the proposed system, the cloud verifies the authenticity of the server without knowing the user's identity before storing data. The paillier cryptosystem also has the added feature of access control in which only valid users are able to decrypt the stored information. The paillier cryptosystem prevents replay attacks and supports creation, modification, and reading data stored in the cloud. Moreover, authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized.

In this project the attributes and access policy of the users are hidden, so the security is high. In this project asymmetric key concept is used for encryption and decryption, so the security is high compared to the other project. Recently, Lewko and Waters [7] proposed a fully decentralized ABE where users could have zero or more attrributes from each authoity and did not require a trusted server.Yan et al. [5] presented a modification of [16], authenticate users who want to remain anonymous while accessing the cloud. To perform anonymous user authentication Attribute Based Signatures were introduced by Maji et al. [11].

And also in this project encryption and decryption is done by means of paillier encryption algorithm. Signature is generated by means of Secure Hash Algorithm. Public key and private key is generated by paillier encryption algorithm. Token is generated by Secure Hash Algorithm. The proposed architecture is given below,

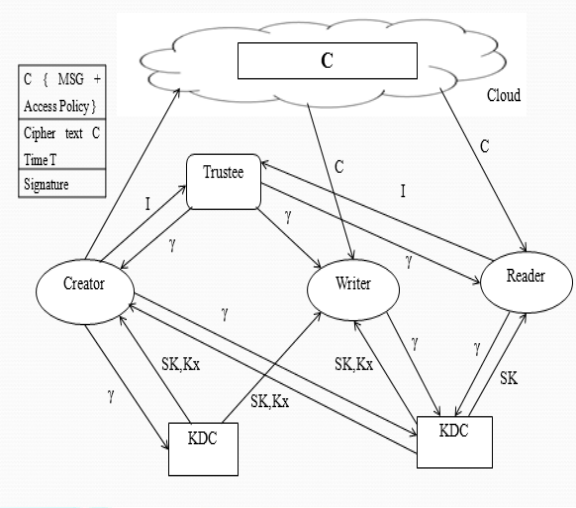

Fig. 1. Secure cloud storage model

In this section privacy preserving authenticated access control scheme is presented. A user can create a file and store it securely in the cloud. In the Fig. 1. There are three users (Creator, Writer, Reader). Users have an initial level Registration Process at the web end. The users provide their own personal information for this process. The server in turn stores the information in its database.

Users receive a token from the trustee, who is assumed to be honest. A trustee can be someone like the federal government who manages social insurance numbers etc. On presenting their id (like health/social insurance number), the trustee gives their a token. There are multiple KDCs, which can be scattered. Users on presenting the token to KDC receive keys for encryption/decryption and signing.

Here the encryption and decryption is done by means of paillier encryption algorithm. And also the public key and the private key is generated by means of KDC.SK are secret keys given for decryption, Kx are keys for signing. χ be a access policy. After the key was received by the User, the message is encrypted by means of the access policy.

The access policies decide who can access the data stored in the cloud. The cipher text C with signature is c, and is sent to the cloud. The cloud verifies the signature and stores the cipher text C. When a reader wants to read, the cloud sends C. If the user has attributes matching with access policy, it can decrypt and get back original message. From a technical point

of view, eyeOS is a platform for web applications, created with the idea to make easy the application development.There are currently a lot of web-related technologies, such as PHP, XHTML, CSS and JavaScript, so it is required to master a lot of languages and understanding numerous concepts to be able to create web applications. eyeOS intends to cover those and other problems derived from the web development, offering the programmers a homogeneous platform to develop their web applications, using only PHP code and leaving to the system the resource management, the communication with the browser, the security, etc.

A. User Enrollment and Signature generation

In this data storage section all the users are give their own information to the trustee. Based on the information the trustee generate the token.The token consists of the following things $\gamma = (u, K_{base}, K_0, \rho)$, where ρ is the signature. KDC only generate the PK[i] and SK[i], they are used for encryption and decryption. And also KDC generate the ASK[i] and APK[i], they are used for signing a verifying. Then the user creates an access policy χ by means of boolean function. For example of boolean function is $(((x_1 \wedge x_2 \wedge x_3) \vee (x_4 \wedge x_5)) \wedge (x_6 \vee x_7))$, where x_1, x_2, ..., x_7 are attributes. The message is then encrypted under the access policy as

C = Paillier. Encrypt (Message, χ)

And also in this scheme time stamp (t) is used. Time stamp is used to prevent the replay attacks. In this scheme a writer whose rights have been revoked cannot create a new signature with new time stamp and thus cannot write back stale information. Signing the message and calculates the message signature as

σ = Paillier.Sign(Public key of trustee, Public key of KDCs, token, Signing Key, message, access claim)

Users have an initial level Registration Process at the web end. The users provide their own personal information for this process. The server in turn stores the information in its database. Users receive a token from the trustee, who is assumed to be honest.

B. Data storage in clouds

The cloud receiving the information verifies the access claim using the algorithm paillier.verify. If the authentication is failed the message is discarded.else the message (C,t) is stored in the cloud. Users presenting the token to KDC and receive keys for encryption and decryption. After the key was received by the User, the message MSG is encrypted under the access policies. And also the message is encrypted by means of secret keys, that is generated by KDC.The access policies decide who can access the data stored in the cloud.The cipher text C with signature is c, and is sent to the cloud.

Paillier algorithm is a probabilistic asymmetric algorithm for public key cryptograpy. The technique used in public key cryptography is the use of asymmetric key algorithms, where the key used to encrypt a message is not the same as the key used to decrypt it. Each user has a pair of cryptographic keys a public key and a private key. The private key is kept secret, whilst the public key may be widely distributed. Messages are encrypted with the recipient's public key and can only be decrypted with the corresponding private key. The steps are given below,

Algorithm: Paillier encryption algorithm

Set n = p×q, p and q are primes
Φ(n) = (p-1)(q-1) – Euler's Totient
λ(n) = lcm(p-1, q-1) – Carmichael's function
Take 2 large primes: p and q randomly and independently of each other. p and q must satisfy condition gcd (p × q , (p − 1)(q − 1)) = 1.
Compute n = p × q and λ = lcm (p -1, q -1);
Select random integer g where
Ensure n divides the order of g. Check the existence of the μ – the modular multiplicative inverse :
Set n = p×q, p and q are primes
Φ(n) = (p-1)(q-1) – Euler's Totient
λ(n) = lcm(p-1, q-1) – Carmichael's function
Take 2 large primes: p and q randomly and independently of each other. p and q must satisfy condition gcd (p × q , (p − 1)(q − 1)) = 1.
Compute n = p × q and λ = lcm (p -1, q -1);
Select random integer g where g ϵ Z*n2!.
Ensure n divides the order of g. Check the existence of the μ – the modular multiplicative inverse :

$$\mu = \left(L\left(g^{\lambda} \bmod n^2\right)\right)^{-1} \bmod n$$

Encryption
Let m be a message to be encrypted where $m \in Z_n$
Select random r where $r \in Z_n^*$
Compute cipher text as: $c = g^m . r^n \bmod n^2$

Decryption

Cipher text $c \in Z_n^*2$

Compute message :$m = L(c^{\lambda} \, mod \, n^2).\mu \, mod \, n$

Based on this algorithm only the encryption and decryption process is done in our project. After the encryption is done the cipher text is stored in the cloud.

C. Data access control

When a reader wants to read, the cloud sends C. If the user has attributes matching with access policy, it can decrypt and getback original message. Write proceeds in the same way as file creation. By designating the verification process to the cloud, it relieves the individual users from time consuming verifications. When a reader wants to read some data stored in the cloud, it tries to decrypt it using the secret keys it receives from the KDCs. If it has enough attributes matching with the access policy, then it decrypts the information stored in the cloud.

3. Comparison Analysis

Compare paillier cryptosystem with other access control schemes and show that this scheme supports many features that the other schemes did not support. 1-W-M-R means that only one user can write while many users can read. M-W-M-R means that many users can write and read. Most schemes do not support many writes which is supported by this scheme. This scheme is robust and decentralized, most of the others are centralized. This scheme also supports privacy preserving authentication, which is not supported by others.

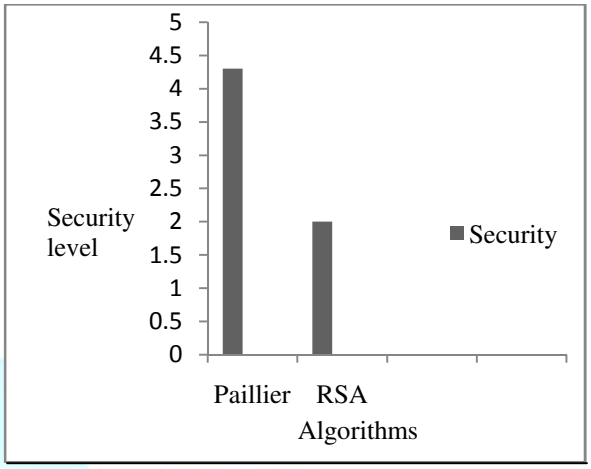

Fig. 2. Comparision of security between paillier and RSA algorithm

Most of the schemes do not support user revocation, which this scheme does. In this scheme all the attributes and access policy is hidden so the security is very high compared to the existing scheme. In this scheme asymmetric key is used for encryption and decryption so the security is high compare to the other schemes. This is shown in the Fig. 2. Compare the computation and communication costs incurred by the users and clouds and show that this distributed approach has comparable costs to centralized approaches. The most expensive operations involving pairings and is done by the cloud. While comparing the computation load of user during read, paillier cryptosystem scheme has comparable cost.

4. Conclusion

A decentralized access control technique with anonymous authentication is presented, which provides user revocation and prevents replay attacks. The cloud does not know the identity of the user who stores information, but only verifies the user's credentials. Key distribution is done in a decentralized way. In this project the attributes and access policy of the users are hidden, so the security is high. In future, the efficiency of uploading data in cloud may also be improved.

References

[1] Sushmita Ruj, Milos Stojmenovic, Amiya Nayak, "Decentralized Access Control with Anonymous Authentication of data stored in Clouds", in *IEEE,* 2013.

[2] Boneh, Dan, Giovanni Di Crescenzo, Rafail Ostrovsky, et Giuseppe Persiano. "Public Key Encryption with Keyword Search ", *Advances in Cryptology - EUROCRYPT 2004.* Springer, 2004. 506-522.

[3] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation,Stanford University, 2009, http: //www. crypto. stanford.

[4] S. Kamara and K. Lauter, "Cryptographic cloud storage," in *FinancialCryptography Workshops*, ser. Lecture Notes in Computer Science, vol.6054. Springer, pp. 136–149, 2010.

[5] Kan Yang, Xiaohua Jia and Kui Ren, " DAC-MACS: Effective Data AccessControl for Multi-Authority Cloud Storage Systems", IACR Cryptology ePrint Archive, 419, 2012.

[6] D. R. Kuhn, E. J. Coyne, and T. R. Weil, "Adding attributes to role-based access control," *IEEE Computer*, vol. 43, no. 6, pp. 79–81, 2010.

[7] A. B. Lewko and B. Waters, "Decentralizing attribute-based encryption," in *EUROCRYPT*, ser. Lecture Notes in Computer Science, vol. 6632. Springer, pp. 568–588, 2011.

[8] M. Li, S.Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multiownersettings," in *SecureComm*, pp. 89–106, 2010.

[9] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in *IEEE INFOCOM*. , pp. 441–445, 2010.

[10] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-based authentication for cloudcomputing," in *CloudCom*, ser. Lecture Notes in Computer Science, vol. 5931. Springer, pp. 157–166, 2009.

[11] H. K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-based signatures:Achieving attribute-privacy and collusion-resistance," *IACR Cryptology ePrint Archive*, 2008.

[12] Matthew Green, Susan Hohenberger and Brent Waters, "Outsourcing the Decryption of ABE Ciphertexts," in USENIX Security Symposium, 2011.

[13] R. C. Merkle, "Protocols for public key cryptosystems," in *Proc.of IEEE Symposium on Security and Privacy*, Los Alamitos, CA, USA, 1980.

[14] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed access control in clouds," in *IEEE TrustCom*, 2011.

[15] A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token-based cloud computing,"in *TRUST*, ser. Lecture Notes in Computer Science, vol. 6101. Springer, pp. 417–429, 2010. edu/craig.

[16] W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and efficient accessto outsourced data," in *ACM Cloud Computing Security Workshop (CCSW)*, 2009.

[17] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-graineaccess control in cloud storage services," in *ACM CCS*, , pp.735–737, 2010.

[18] C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing", *IEEE T. Services Computing*, vol. 5, no. 2, pp. 220–232, 2012.

[19] F. Zhao, T. Nishide, and K. Sakurai, "Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems," in *ISPEC*, ser. Lecture Notes in Computer Science, vol. 6672. Springer, pp. 83–97, 2011.