ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

An ISO 3297: 2007 Certified Organization Vol.3, Special Issue 4, April 2015

National Conference On Emerging Trends in Information, Digital & Embedded Systems (NC'e-TIDES -15)

Organized by

Dept. of ECE, Annamacharya Institute Of Technology & Sciences, Rajampet, Andhra Pradesh-516126, India held on 28th February 2015

Key Distribution Centre with Privacy Preserving Authentication Data Storage in Clouds

Avula Madhu Kiran, Mahesh Mahanandi, M.Rudrakumar

Student in A.I.T.S, Dept. of C.S.E, Rajampet, JNTUA University, Anantapur. India

Student in G.T.E.S, Dept of C.S.E,JNTUH Univercity, Hyderabad, India

Associate professor in A.I.T.S, Rajampet, JNTUA University, Anantapur, India

ABSTRACT: It propose a new decentralized access control scheme for secure data storage in clouds that supports anonymous authentication. It proposed the cloud verifies the authenticity of the series without knowing the user's identity before storing data. The scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. It also address user revocation. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. The communication, computation, and storage overheads are comparable to centralized approaches.

KEYWORDS: Access control, authentication, attribute-based signatures, attribute-based encryption, cloud storage.

I. INTRODUCTION

Research In Cloud Computing Is Receiving A Lot Of Attention From Both Academic And Industrial Worlds.In Cloud Computing, Users Can Outsource Their Computation And Storage To Servers (Also Called Clouds) Using Internet. This Frees Users From The Hassles Of Maintaining Resources On-Site. 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).

Much of the data stored in clouds is highly sensitive, for example, medical records and social networks. Security andprivacy 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. The cloud can hold the user accountable for the data it outsources, and likewise, the cloud is itself accountable for the services it provides. The validity of the user who stores the data is also verified. Apart from the technical solutions to ensure security and privacy, there is also a need for law enforcement.

Considering the following situation: A law student, Alice, wants to send a series of reports about some malpractices by authorities of University X to all the professors of University X, research chairs of universities in the country, and students belonging to Law department in all universities in the province.She wants to remain anonymous while publishing all evidence of malpractice. She stores the information in the cloud. Access control is important in such case, so that only authorized users can access the data. It is also important to verify that the information comes from a reliable source. The problems of access control, authentication, and privacy protection should be solved simultaneously

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

An ISO 3297: 2007 Certified Organization Vol.3, Special Issue 4, April 2015

National Conference On Emerging Trends in Information, Digital & Embedded Systems (NC'e-TIDES -15)

Organized by

Dept. of ECE, Annamacharya Institute Of Technology & Sciences, Rajampet, Andhra Pradesh-516126, India held on 28th February 2015

II. RELATED WORK

ABE was proposed by Sahai and Waters [3]. In ABE, a user has a set of attributes in addition to its unique ID. There are two classes of ABEs. In key-policy ABE or KP-ABE (Goyal et al. [4]), the sender has an access policy to encrypt data. A writer whose attributes and keys have been revoked cannot write back stale information. The receiver receives attributes and secret keys from the attribute authority and is able to decrypt information if it has matching attributes. In Ciphertext-policy, CP-ABE ([5], [6]), the receiver has the access policy in the form of a tree, with attributes as leaves and monotonic access structure with AND, OR and other threshold gates.All the approaches take a centralized approach and allow only one KDC, which is a single point of failure. Chase [7] proposed a multiauthority ABE, in which there are several KDC authorities (coordinated by a trusted authority) which distribute attributes and secret keys to users.

Multiauthority ABE protocol was studied in [8] and [9], which required no trusted authority which requires every user to have attributes from at all the KDCs. Recently, Lewko and Waters [10] proposed a fully decentralized ABE where users could have zero or more attributes from each authority and did not require a trusted server. In all these cases, decryption at user's end is computation intensive. So, this technique might be inefficient when users access using their mobile devices. To get over this problem, Green et al. [11] proposed to outsource the decryption task to a proxy server, so that the user can compute with minimum resources (for example, hand held devices). However, the presence of one proxy and one KDC makes it less robust than decentralized approaches. Both these approaches had no way to authenticate users, anonymously. Yang et al. presented a modification of , authenticate users, who want to remain anonymous while accessing the cloud. To ensure anonymous user authentication ABSs were introduced by Maji et al. [1]. This was also a centralized approach. A recent scheme by Maji et al. [1] takes a decentralized approach and provides authentication without disclosing the identity of the users. However, as mentioned earlier in the previous section it is prone to replay attack.

III. PROPOSED ALGORITHM

SYSTEM INITIALIZATION

Select a prime q, and groups G1 and G2, which are of order q. We define the mapping ˆe : G1 ×G1 . G2. Let g1, g2 be generators of G1 and hj be generators of G2, for j . [tmax], for arbitrary tmax. Let H be a hash function. Let A0 = ha0 0 , where a0 . Z* q is chosen at random. (TSig,TV er) mean TSig is the private key with which a message is signed and TV er is the public key used for verification. The secret key for the trustee is TSK = (a0, TSig) and public key is TPK = (G1,G2,H, g1,A0, h0, h1, . . . , htmax, g2, TV er).

User Registration

For a user with identity Uu the KDC draws at random Kbase . G. Let K0 = K1/a0 base . The following token . is output . = (u,Kbase,K0, .), where . is signature on u||Kbase using the signing key TSig.

KDC setup

We 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. The architecture is decentralized, meaning that there can be several KDCs for key management.

Attribute generation

The token verification algorithm verifies the signature contained in . using the signature verification key TV er in TPK. This algorithm extracts Kbase from . using (a, b) from ASK[i] and computes Kx = K1/(a+bx) base , x . J[i, u]. The key Kx can be checked for consistency using algorithm ABS.KeyCheck(TPK,APK[i], .,Kx), which checks ˆe(Kx,AijBx ij) = ˆe(Kbase, hj), for all x . J[i, u] and j . [tmax].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

An ISO 3297: 2007 Certified Organization Vol.3, Special Issue 4, April 2015

National Conference On Emerging Trends in Information, Digital & Embedded Systems (NC'e-TIDES -15)

Organized by

Dept. of ECE, Annamacharya Institute Of Technology & Sciences, Rajampet, Andhra Pradesh-516126, India held on 28th February 2015

Sign

The access policy decides who can access the data stored in the cloud. The creator decides on a claim policy Y, to prove her authenticity and signs the message under this claim. The ciphertext C with signature is c, and is sent to the cloud. The cloud verifies the signature and stores the ciphertext 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.

Verify

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.

IV. PSEUDO CODE

Step1: The file can be stored in clouds by using encrypted algorithm.
Step2: The encryption process Select a prime q,and groups G1 and G2,which order q .
Step3:The valid user can access the data by using secret key .
Step4: Anonymous person can store data and valid users can access data by decryption process.
Step5: Calculate the overhead from G1 and G2 change when larger size of data is stored .

Simulation Results

The simulation can be implemented by using the 3 users, a creator,a reader, and a writer can be represented by using the following fig 1. Creator Alice receives 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 her id (like health/social insurance number), the trustee gives her a token ∞. There are multiple KDCs (here 2), which can be scattered. For example, these can be servers in different parts of the world. A creator on presenting the token to one or more KDCs receives keys for encryption/decryption and signing.

In the Fig. 1, SKs are secret keys given for decryption, Kx are keys for signing. The message MSG is encrypted under the access policy X. The access policy decides who can access the data stored in the cloud. The creator decides on a claim policy Y, to prove her authenticity and signs the message under this claim.

The ciphertext C with signature is c, and is sent to the cloud. The cloud verifies the signature and stores the ciphertext 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. 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

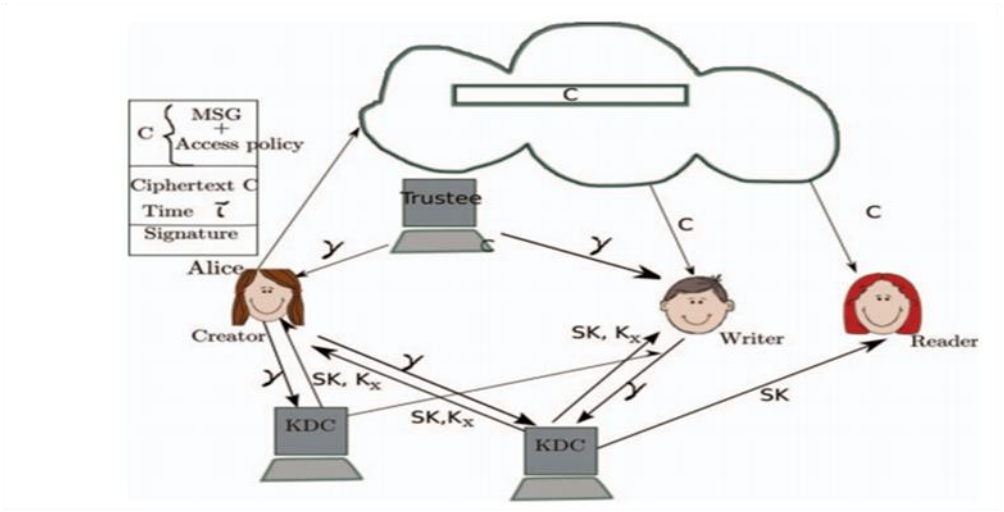
An ISO 3297: 2007 Certified Organization *Vol.3, Special Issue 4, April 2015*

National Conference On Emerging Trends in Information, Digital & Embedded Systems (NC'e-TIDES -15)

Organized by

Dept. of ECE, Annamacharya Institute Of Technology & Sciences, Rajampet, Andhra Pradesh-516126, India held on 28th February 2015

SYSTEM ARCHITECTURE



V. CONCLUSION AND FUTURE WORK

The simulation results showed that presented a decentralized access control technique with anonymous authentication, which provides user revocation and prevents replay attacks. The cloud does not know the identity of the user who stores in formation,but only verifies the user's credentials. Key distribution is done in a decentralized way. One limitation is that the cloud knows the access policy for each record stored in the cloud. In future, we would like to hide the attributes and access policy of a user.

REFERENCES

1. Avula Madgu Kiran, M.Mahesh,and M.Rudra Kumar '**Key distribution centre with privacy preserving authentication data storage in clouds'** –A Survey', International Journal of Emerging Trends & Technology in computer Science, Vol.3, Issue 1, pp. 218-223, 2015.
2. H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures," Topics in Cryptology - CT-RSA, vol. 6558, pp. 376-392,2011
3. A. Beimel, "Secure Schemes for Secret Sharing and Key Distribution," PhD thesis, Technion, Haifa, 1996.
4. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc .Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 457-473, 2005.
5. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006.
6. J. Bethen court , A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.
7. X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably Secure and Efficient Bounded Ciphertext Policy Attribute Based Encryption," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp 343-352, 2009.
8. M. Chase, "Multi-Authority Attribute Based Encryption," Proc. Fourth Conf. Theory of Cryptography (TCC), pp. 515-534, 2007.
9. H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure Threshold Multi-Authority Attribute Based Encryption without a Central Authority," Proc. Progress in Cryptology Conf. (INDOCRYPT), pp. 426-436, 2008.
10. M. Chase and S.S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proc. ACM Conf. Computer and Comm. Security, pp. 121-130, 2009.
11. M. Green, S. Hohenberger, and B. Waters, "Outsourcing the Decryption of ABE Ciphertexts," Proc. USENIX SecuritySymp.,2011.
12. K. Yang, X. Jia, and K. Ren, "DAC-MACS: Effective Data Access Control for Multi-Authority Cloud".

BIOGRAPHY

Avula MadhuKiran is a Research Assistant in the Computer Science & Engineering Department, College of Annamacharya Institute of Technology and Science, JNTUA University. He received Master of Technology post graduation in 2015 from JNTUA, Ananthapur, India. His research interests are Cloud Computing .