Cryptographic Approaches for Data Assurance in Cloud

B Saritha[1], More Praveen[2]

[1,2]*Assistant Professor, Department of Computer Science and Engineering*
[1,2]*Malla Reddy Engineering College (A), Hyderabad, Telangana, India.*

Abstract

The main objective of this system is to develop an experimental model to store the data securely in cloud computing environment and provides high level of trustworthy data maintenance scheme to its users with Advanced Cryptographic Standards (ACS) scheme. In this system a novel proof based trustworthy data management scheme to upload the data into the server with proper cryptographic principles such as Advanced Cryptographic Standards (ACS), with these systems the data owner and data users is successfully maintain and retrieve the data to and from the server. Authentication is the procedure to ensure the cloud data in a secured manner. The strong user authentication is the main requirement for cloud computing that reduces the unauthorized user access of data on cloud. Data security is most important issue of cloud computing. Role-based access control (RBAC) method controls access to computer or network environmental based on the roles given to individual users within an organization. Roles are defined according to job skill, authority, and responsibility within an organization. In RBAC roles can be easily created, changed, or discontinued as the needs of an organization involve, without updating the privileges for every user. We propose a new Secure Cloud Data to enhancement the framework model in data security and cloud storage model by integrating the dual system encryption technology with selective proof technique.

Index Terms: *Data-Centric Security, Cloud Computing, Role-Based Access Control, Authorization. Cryptography, Encryption, Decryption, Cipher Text,*

1. Introduction

Security is one of the main user concerns for the adoption of Cloud computing moving data to the cloud usually implies relying on the Cloud Service Provider (CSP) for data protection [1]. Although this is usually managed based on Service Level Agreements (SLA), the CSP could potentially access the data is provided to third parties. Moreover, one should trust the CSP to legitimately apply the access control method defined by the data owner for other users [2]. Advanced Cryptographic Standard to secure the data re-encrypts data from one key to another without getting access and to use identities in cryptographic model[3]. Each piece of data is ciphered with its own encryption key linked to the authorization model and rules are cryptographically security to preserve data against the service provider access to evaluating the rules [4]. Security is important information to a platform which is not directly controlled by the user and which is far away [5]. The sending of data and during storage data is under threat because any unauthorized user can access it modify it so there is need to secure data. A data is secure, if it fulfils three conditions (i) Confidentiality (ii) Integrity (iii) Availability. it helps in preventing the unauthorized disclosure of sensitive information. Integrity means data received by receiver should be in the same form the sender sends it integrity helps in preventing modification from unauthorized user [6]. Role-based access control model has three essential structures users' permissions and roles. A role is a higher-level representation of access control [7]. User corresponds to real world users of the computing system. User authorization is accomplished separately; assigning users to backend roles and assigning access privileges for objects to roles. Permissions gives a description of the access users can have to objects in the system and roles gives a description of the functions of users [8]. Data duplication enables data storage systems to find and remove duplication within data without compromising its availability. The goal of data duplication is to store more data in small space by storing and maintaining into a single copy the redundant copies of data are replaced [9].

Copyright © 2020 Authors

2. Related Work

Cloud Computing is large collection of interconnected network. There are so many associated with the cloud network like data is hacked by an unauthorized person. Data can be changed by third party while transferring [10]. The main issues related to data security include data integrity data availability, data confidentiality, privacy, transparency of data and control over data [11]. There are many aspects for providing data security such as by providing access controls and encryption methods. The service provider must security infrastructure that providing is secure and client's data remain protected [12]. A cryptographic scheme that enables an entity called re-encrypt data from one key to another without being able to decrypt it. A couple of key pairs and proxy could re-encrypt a cipher text encrypted under public key to another cipher text is decrypted using private key using this kind of cryptography [13]. We present new techniques for realizing Cipher text-Policy Attribute Encryption (CP-ABE) under concrete and cryptographic assumptions in the standard model. Our solutions access encrypted to specify access control in terms of any access formula over the attributes in the system. In our most efficient system cipher text size, encryption, and decryption time scales linearly with the complexity of the access formula [14]. The first method is avoid using tags that are derived deterministically from the message [16]. They designed a fully randomized scheme that supported equality test over cipher text. There main components in the fully randomized scheme, namely a payload, a tag and a proof of consistency [15].

3. System Architecture

A secure RBAC based on hybrid cloud storage system to allows an organization to store information on public cloud and maintain sensitive data on private cloud. Public cloud provides services in a virtualized environment constructed using pooled shared physical resources, and accessible over a public network [17]. Third Party Auditors (TPAs) and SUB TPAS clients is those data to stored and accessing the data with help of Cloud Service Provider (CSP). They are many desktop computers, laptops, mobile phones, tablet computers [18].

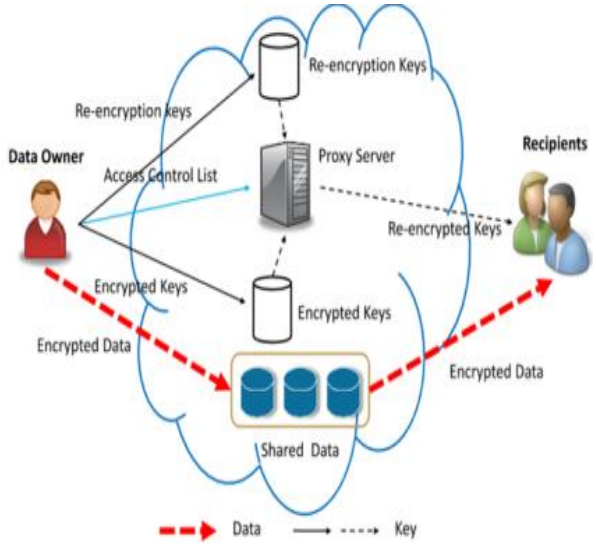

Figure 1. Proposed System Architecture

We first provide the basic RDPC scheme only for static data integrity checking. Furthermore, we show the advanced RDPC scheme supporting fully dynamic block operations based on ORT. A. Basic RDPC Scheme We use the homomorphism hash function defined to construct our basic RDPC scheme system [19]. Components and its Security consists of six algorithms namely Setup, Extract, Tag Gen, Challenge, Proof Gen and Proof Check are involved in a CP-ABPRE system. Administrators generate the system parameters. System parameters represent the position of the role and stored that role in private cloud. Administrators manage role hierarchy. Role manager manages role for users [20]. According to the role, user gets access permission to data. Each role has different parameters associated with it

Copyright © 2020 Authors

3.1. RSA (Rivest-Shamir-Adleman)

This is an Internet encryption and authentication system that uses an algorithm developed in 1977. The RSA algorithm is the most commonly used encryption. Till now it is the only algorithm used for private and public key generation and encryption. It is a fast encryption [23]

Algorithm

1. Key Generation: KeyGen(p, q)
2. Input: Two large primes –p, q
3. Compute n = p. q
4. φ (n) = (p -1) (q -1)
5. Choose e such that gcd(e, φ (n)) = 1
6. Determine d such that e.d ≡ 1 mod φ (n)
7. Key:
8. Public key = (e, n)
9. Secret key= (d, n)
10. Encryption: c = me mod n where c is the cipher text and m is the plain text

RSA has a multiplicative homomorphism property it is possible to find the product of the plain text by multiplying the cipher texts. The result of the operation will be the cipher text of the product. Given ci = E (mi) = mie mod n, then (c1. c2) mod n = (m1 . m2)e mod n.

3.1.1. Key Distribution

In key distribution is the TPA generates the random key and distributes it to his CP-ABPRE as follows: The TPA first generates the Random key by using SOBOL Random Function. After that TPA chooses CP-ABPRE and distributes n pieces to them. The procedure of key distribution is given in algorithm [21].

Algorithm: Key Distribution

1. Generates a random key K using SOBOL Sequence

   K= f* I* k

2. Then, the TPA partition the K into n pieces using (m, n) secret sharing scheme

3. TPA select the Number of SUBTPAs : n, and threshold value m;

4. for I=1 to n do

5. TPA sends KI to the all SUBTPAI s

6. end for

7. end

In verification model total SUBTPAs verify the Integrity of data and give results to the TPA; if SUBTPAs responses meet the threshold value then TPA says that Integrity of data is valid. At a high level, the protocol operates like TPA assigns a local timestamp to every SUBTPA of its operations [22]. Hellman key modify method access two parties that have no prior knowledge of each other to jointly establish destitutions secret key over an insecure communications channel. This key can then be used to encrypt subsequent communication using a symmetric key cipher text.

4. Experiment Results

We mainly analyze the computation cost of PEKS models trapdoor generation and testing in the schemes of our scheme. The computation cost of our scheme is only slightly higher than that of the BCOP scheme in terms of PEKS generation and trapdoor generation. To be more precise the time of trapdoor generation for 50 keywords is about 0.12 seconds while that of our scheme is 0.08 seconds. Regarding the testing operation the computation cost is almost many our scheme. Specifically, the computation cost of testing is around 1.6 second for the scheme and 0.8 seconds for our scheme. This is because the testing requires an additional pairing computation.

 Copyright © 2020 Authors

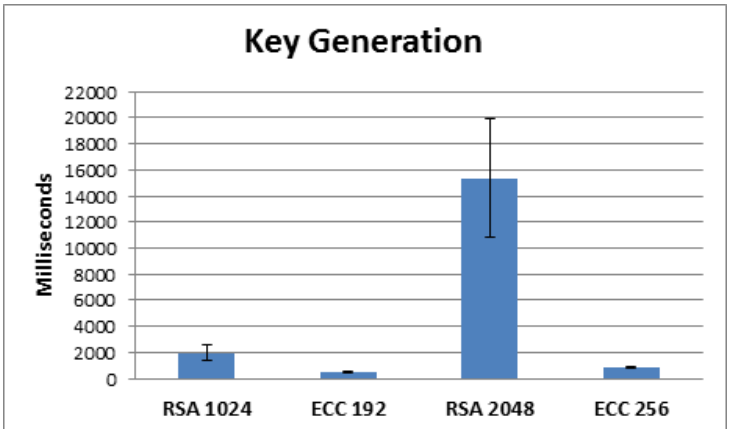

Figure 2. Key Generation

5. Conclusion

Cloud Computing model very useful service for many people; every third person is using cloud in different ways. Due to its flexibility, many persons are transferring their data to cloud. Guidelines for deployment in a Cloud Service Provider are also given, including a hybrid model compatible with Public Key Cryptography that enables the usage of standard PKI for key management and distribution. Role-based access control model based on hybrid cloud storage architecture in which encrypted data is stored on public cloud and sensitive information related to organization stored on private cloud, from which outside users can not access data directly. The security as a service model while proffering a baseline security measures to the provider to save from harm its own cloud infrastructure also make available of flexibility to tenants and have supplementary precautions functionalities is costume their security necessities. The future work would is test the tool on real prospective cloud consumers to check if it can effectively help with cloud provider selection.

References

[1] Cloud Security Alliance, “Security guidance for critical areas of focus in cloud computing v3.0,” CSA, Tech. Rep., 2003.

[2] Y. Zhang, J. Chen, R. Du, L. Deng, Y. Xiang, and Q. Zhou, “Feacs: A flexible and efficient access control scheme for cloud computing,” in Trust, Security and Privacy in Computing and Communications, 2014 IEEE 13th International Conference on, Sept 2014, pp. 310–319.

[3] B. Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in Public Key Cryptography - PKC 2011, 2011, vol. 6571, pp. 53–70.

[4] B. B and V. P, “Extensive survey on usage of attribute based encryption in cloud,” Journal of Emerging Technologies in Web Intelligence, vol. 6, no. 3, 2014.

[5] Anitha Y, “Security Issues in cloud computing”, “International Journal of Thesis Projects and Dissertations “(IJTPD) Vol. 1, Issue 1, PP :(1-6), Month: October 2013.

[6] Qi. Zhang ·Lu. Cheng, Raouf Boutaba, “Cloud computing: state-Of-the-art and research Challenges”, “The Brazilian Computer Society”, April 2010

[7] Zahir Tari and Shun-Wu Chan “Role-based access control for intranet security”, IEEE Internet Computing, Vol. 1, No. 4, September 1997

[8] Pierangela Samarati and Sabrina de Capitani di Vimarcati “Access control: Policies, Models and Mechanism”, 2001

[9]. M. Storer, K. Greenan, D. Long, and E. Miller, “Secure data de duplication,” in Proc. of the 4th ACM International Workshop on Storage Security and Survivability, VA, USA, Oct. 2008, pp. 1–10

[10] Garima Saini, Gurgaon Naveen Sharma,”Triple Security of Data in Cloud Computing “, Garima Saini

Copyright © 2020 Authors

[11] Yogesh Kumar, Rajiv Munjal and Harsh Sharma,"Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures" IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011.

[12] D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud ,"Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA Volume 8, 2009.

[13] E. Coyne and T. R. Weil, "Abac and rbac: Scalable, flexible, and auditable access management," IT Professional, vol. 15, no. 3, pp. 14–16, 2013.

[14] Empower ID, "Best practices in enterprise authorization: The RBAC/ABAC hybrid approach," Empower ID, White paper, 2013.

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

[16]. M. Abadi, D. Boneh, I. Mironov, A. Raghunathan, and G. Segev, "Message-locked encryption for lockdependent messages," in CRYPTO 2013, ser. Computer Science, R. Canetti and J. A. Garay, Eds. Springer, 2013, vol. 8042 of LNCS, pp. 374–391.

[17]. R. A. Popa, C. M. S. Redfield, N. Zeldovich, and H. Balakrishnan, "Cryptdb: Protecting confidentiality with encrypted query processing," in Proc. of ACM Symposium on Operating Systems Principles, Cascais, Portugal, Oct. 2011, pp. 85–100.

[18]. R. A. Popa, F. Li, and N. Zeldovich, "An ideal-security protocol for order-preserving encoding," in Proc. of IEEE Symposium on Security and Privacy, CA, USA, May 2013, pp. 463–477.

[19]Y. Zhu, D. Ma, C. Hu, and D. Huang, "How to use attribute-based encryption to implement role-based access control in the cloud," in Proc. Int. Workshop Sec. Cloud Comput., 2013, pp. 33–40.

[20]A. Shamir, "Identity-based cryptosystems and signature schemes," in CRYPTO (Lecture Notes in Computer Science), vol. 196. New York, NY, USA: SpringerVerlag, 1984, pp. 47–53

[21]. J. Douceur, A. Adya, W. Bolosky, D. Simon, and M. Theimer, "Reclaiming space from duplicate files in a server less distributed file system," in Proc. of IEEE International Conference on Distributed Computing Systems, Macau, China, Jun. 2002, pp. 617–624.

[22]. D. Harnik, B. Pinkas, and A. Shulman-Peleg, "Side channels in cloud services: De duplication in cloud storage," in Proc. of IEEE Symposium on Security and Privacy, CA, USA, Jan. 2010, pp. 40–47

[23] Uma Somani, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing,"2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC-2010).

Copyright © 2020 Authors