International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Attribute-Based Access Control Scheme for Security of Cloud Storage Systems Using RNS Cryptography

Priya Thomas

M. Tech, Department of Computer Science Engineering, MVJCE, Bangalore-56, India

Abstract: ***Emerging features of the cloud storage services enables data owners to store their big data in the cloud and provide the data access to the users. As privacy and security of the cloud server is not ensured, an Attribute-Based Encryption (ABE) a promising technique for data access control in cloud storage is utilized in this project. Attribute-based encryption, especially for cipher text-policy attribute-based encryption, can fulfil the functionality of fine-grained access control in cloud storage systems. In the proposed scheme, any user can recover the outsourced data if and only if this user holds sufficient attribute secret keys with respect to the access policy and authorization key in regard to the outsourced data. Both the size of cipher text and the number of pairing operations in decryption are constant, which reduce the communication overhead and computation cost of the system. Residue Number Systems (RNS) are useful for distributing large dynamic range computations over small modular rings, which allows the speed up of computations. RNS algorithm will be used for the encryption and decryption process involved, which can be used to achieve performance improvement as the arithmetic involves smaller numbers and can be done in parallel. This ensures the system is very fast, most reliable and is executed with the least computational costs.***

Keywords: Attribute-based encryption, two-factor protection, user-level revocation

1. Introduction

The current day multi-authority attribute-based cloud systems are either insecure in attribute-level revocation or lack of efficiency in communication overhead and computation cost. As the cloud servers cannot be fully trusted and may attempt to access user data for illegal purpose, the concern about data security and privacy arises. One common method for alleviating this problem is to store data in encrypted form, which is more important for protecting sensitive user data. However, this brings forth new challenges: how to realize access control over encrypted data that is, sharing confidential data on cloud servers [1], [10].

Currently, role-based access control (RBAC) model is the most popular model used in enterprise systems; however, this model has severe security problems when applied to cloud systems. A classic RBAC model uses reference monitors running on data servers to implement authorization. However, the servers in the cloud are out of the control of enterprise domains and, therefore, must be considered untrusted by default. Hence, building an effective data protection mechanism for cloud-based enterprise systems has become a major challenge [2], [10]. As sensitive data may be stored in the cloud for sharing purpose or convenient access; and eligible users may also access the cloud system for various applications and services, user authentication has become a critical component for any cloud system [3].

In most existing schemes, the size of ciphertext linearly grows with the number of attributes involved in the access policy [10], which may incur a large communication overhead and computation cost. This will limit the usage of resource-constrained users. The attribute-level revocation is very difficult since each attribute is conceivably shared by multiple users. The proposed scheme provides two-factor protection mechanism to enhance the confidentiality of outsourced data. RNS algorithm will be utilized for the encryption and decryption process involved and which ensures the system is fast, most reliable and is executed with the least computational costs

2. Literature Survey

The criticality and importance of security aspect in cloud storage system is analyzed in various previous surveys. Zechao Liu [1] discussed a dynamic attribute based access control scheme to perform attribute revocation and policy updates and considers multiple attribute authorities in this scheme which can work independently without any cooperation and presence of any central authority.

BO LANG [2]proposes a self-contained protection mechanism for outsourced enterprise data. In addition to being compatible with the existing RBAC system, this method also allows users to specify other required policies for each data object. Hui Ma_, Rui Zhang_, Zhiguo Wan [3] proposes a scheme where in heavy computations are outsourced to Encryption Service Providers (ESPs) or Decryption Service Providers (DSPs), leaving only one modular exponentiation computation for the sender or the receiver.

Jianghong Wei[4] presented a system where a central authority is not required to issue various attributes. Each attribute authority can independently issue relevant keys for the users.Kaiping Xue [5] presented an effective central authority to generate secret keys for the users. An auditing mechanism is proposed to detect which attribute authority has incorrectly or maliciously performed legitimacy verification procedure.

Saraswati Gore1, Ashokkumar Kalal2[6] presented a survey paper explaining the two factor access control policy for multi-authority cloud storage systems. Jiguo Li, Wei Yao [7] proposed a scheme for efficient user collision avoidance. A CP-ABE scheme with efficient attribute revocation is proposed. Pranayanath Reddy Anantula1, 2Dr G Manoj Someswar [8] proposed an OTP based two factor authentication scheme for multi-authority cloud systems.Boyang Wang, Student Member [10] proposed public auditor mechanism for ensuring two factor cloud security.

3. Existing System

Multi-authority attribute-based systems are either insecure in attribute-level revocation or lack of efficiency in communication overhead and computation cost.RSA algorithm is mostly used for the encryption and decryptionEncryption based on bit value and hence slower compared to decimal value based encryptionIn most existing schemes, the size of ciphertext linearly grows with the number of attributes involved in the access policy, which may incur a large communication overhead and computation cost. This will limit the usage of resource-constrained users. More prone to security attacks as the commonly used encryption techniques involved does not support split shares of data

4. Proposed System

The proposed system provides two-factor protection mechanism to enhance the confidentiality and authorization to the outsourced data on cloud servers.

- Attribute-based access control solution ensures that the end user will be authorized via an attribute secret key to the data on cloud server.
- The RNS algorithm encrypts the sensitive data in the cloud

The architecture of proposed system is shown in figure 1.

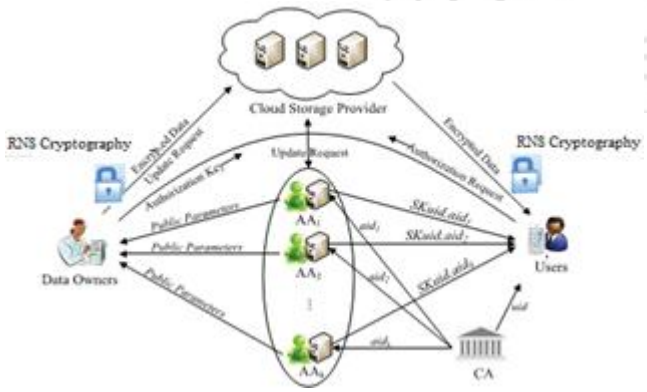

Figure 1: Architecture of Proposed System

The Attribute-based access results in a constant size cipher text decryption and reduces the communication overhead and computation cost of the system. RNS algorithm used for the encryption and decryption optimizes performance as the arithmetic involves decimal value of byte and can be processed in parallel by splitting the encrypted data. The solution supports attribute-level revocation and data owner/administrators can perform user-level revocation.
The framework of the proposed scheme consists of the following phases:

A. Phase 1: System Initialization:
First, the CA generates some global public parameters for the system, and accepts both the AA registration and user registration. Then, each AA and data owner respectively generate the public parameters and secret information used throughout the execution of system.

B. Phase 2: Secret Key and Authorization Generation:
When a user submits a request of attribute registration toAA, the AA distributes the corresponding attribute secret keysto this user if his/her certificate is true*using RNS encryption*. When a user submits anauthorization request to data owner, the data owner generatesthe corresponding authorization key and delivers it to this user.

C. Phase 3: Data Encryption
For each shared data, the data owner first defines an accesspolicy, and then encrypts the data under this specified accesspolicy. Thereafter, the data owner outsources this ciphertextto the CSP. The encryption operation will use a set of publickeys from the involved AAs and the data owner's authorizationsecret keyusing RNS encryption.

D. Phase 3: Data Decryption:
All the users in the system are allowed to query and download any interested cipher texts from the CSP. A user is able to recover the outsourced data, only if this user holds thesufficient attribute secret keys with respect to access policyand authorization key with regard to outsourced data using RNS encryption.

E. Phase 5: User-level Revocation
In order to revoke a user's access privilege, the data owner generates a new authorization secret key used for authorization, a set of authorization update keys for non-revoked users and a set of cipher text update components for cipher text update. When receiving the authorization update key, each non-revoked user updates the authorization key and obtains the new version. All the involved cipher texts will be updated by the CSP based on the set of cipher text update components.

5. Algorithm

In this project we have used RNS (Residue number system) Algorithm. This algorithm having thefollowing:

Step 1: First we have to select two random numbers.
Step 2: Generate the key by using two random numbers.
M = P1 * P2 =143
A1 = M / P1 = 143 / 11 = 13
A2 = M / P2 = 143 / 13 = 11
T Value is, it can be anything
T1 = ((A1 * T) mod P1) == 1
T1 = 6
T2 = ((A2 * T) mod P2) == 1
T2 = 6
Step3: Encrypt the file with help of key.
R1 = N % P1 = 80 % 11 = 3
R2 = N % P2 = 80 % 13 = 2
Step4: Then Decrypt the file
E = [(A1 * T1 * R1) + (A2 * T2 * R2)] mod M
E = [(13 * 6 * 3) + (11 * 6 * 2)] mod 143
E = [234 + 132] mod 143
E = [366] mod 143
E = 80

The above algorithm is known as RNS namely Residue Number System algorithm. By using this algorithm the encryption and decryption processes happened on the given cloud data storage.

6. Results and Discussion

Extensive security analysis, performance comparisons and experimental results indicate that the proposed scheme is suitable to data access control for multi authority cloud storage systems.

7. Conclusion

Cloud is being used widely and it will be used even more in the future which will lead to more storage and sharing of sensitive data via cloud. This calls for improved cloud server security and data-level security. The proposed solution address the need for improved cloud server security and data-level security by using an Attribute-based access control scheme with two-factor protection along with the RNS algorithm to take it the next level. Security should be continuous improvement and needs to be.

References

[1] Zechao Liu∗, Zoe L. Jiang∗†, Xuan Wang∗‡, S.M. Yiu§, Chunkai Zhang∗and Xiaomeng Zhao, Fellow, IEEE, "Dynamic Attribute-Based Access Control in Cloud Storage Systems", 2016 IEEE TrustCom/BigDataSE/ISPA
[2] BO LANG, (Member, IEEE), JINMIAO WANG, AND YANXI LIU, "Achieving Flexible and Self-Contained Data Protection in Cloud Computing," IEEE Access Journal., date of publication February 7, 2017.
[3] Hui Ma_, Rui Zhang_, Zhiguo Wan, Yao Lu and Suqing Lin, "Verifiable and Exculpable Outsourced Attribute-Based Encryption for Access Control in Cloud Computing," IEEE Trans.Knowl. Dependable and Secure Computing, 2015.
[4] Jianghong Wei, Wenfen Liu, and Xuexian Hu "Secure and Efficient Attribute-Based Access Control for Multiauthority Cloud Storagein" IEEE SYSTEMS JOURNAL,2016.
[5] Kaiping Xue, *Senior Member*, *IEEE*, Yingjie Xue, Jianan Hong, Wei Li, Hao Yue, *Member*, *IEEE*, David S.L. Wei, *Senior Member*, *IEEE*, and Peilin Hong, "RAAC: Robust and Auditable Access Control with Multiple Attribute Authorities for Public Cloud Storage," IEEE Transactions on Information Forensics and Security,2017.
[6] Saraswati Gore1, Ashokkumar Kalal2, "A Survey on Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services" International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 10, October 2016
[7] Jiguo Li, Wei Yao, Jinguang Han, *Member, IEEE*, Yichen Zhang, and Jian Shen, "User Collusion Avoidance CP-ABE With Efficient Attribute Revocation for Cloud Storage", IEEE SYSTEMS JOURNAL, 2017.
[8] Pranayanath Reddy Anantula1, 2Dr G Manoj Someswar, "Preserving privacy in Cloud based applications using two-factor authentication (TOTP/WTP)," IJARCCE, Vol. 5, Issue 12, December 2016.
[9] Joseph K. Liu, Man Ho Au_, Xinyi Huang, Rongxing Lu, Jin Li, "Fine-grained Two-factor Access Control for Web-based Cloud Computing Services" IEEE Transactions on Information Forensics and Security,2017.
[10] Boyang Wang, Student Member, IEEE, Baochun Li, Senior Member, IEEE, and Hui Li, Member, IEEE, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud," IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. 8, NO. 1, JANUARY/FEBRUARY 2015.