Attribute-Based Encryption Scheme for Privacy of Cloud Storage through RNS Cryptography

M.VijayaLakshmi, Dept. of CSE,St.Martin's Engineering College, Hyderabad.

D.Navanitha, Dept. of CSE,St.Martin's Engineering College, Hyderabad.

Abstract: Emerging features of the distributed storage administrations empowers information proprietors to store their big data in the cloud and give the information access to the clients. As privacy and security of the cloud server isn't guaranteed, an Attribute-Based Encryption (ABE) a promising system for information get to control in distributed storage is used in this undertaking. Property based encryption, roleicularly for figure content approach quality based encryption, can satisfy the usefulness of fine-grained get to control in distributed storage frameworks. In the proposed plot, any client can recuperate the outsourced information if and just if this client holds adequate property mystery keys as for the entrance strategy and approval enter with respect to the outsourced information. Both the extent of figure content and the quantity of matching operations in unscrambling are consistent, which diminish the correspondence overhead and calculation cost of the framework. Residue Number Systems (RNS) are helpful for dispersing substantial dynamic range calculations over little roleicular rings, which permits the accelerate of calculations. RNS calculation will be utilized for the encryption and unscrambling process included which can be utilized to accomplish execution change as the math includes littler numbers and should be possible in parallel. This guarantees the framework is quick, most dependable and is executed with the minimum computational expenses.

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

1. Introduction

The present day multi-authority quality based cloud frameworks are either unreliable in property level disavowal or absence of effectiveness in correspondence overhead and calculation cost. As the cloud servers can't be completely trusted and may endeavour to get to client information for unlawful reason, the worry about information security and privacy emerges. One regular technique for easing this issue is to store information in encoded frame, which is more essential for securing touchy client information. Be that as it may, this delivers new difficulties: how to acknowledge get to control over encoded information that is, sharing secret information on cloud servers. Presently, role based access control (RBAC) demonstrate is the most mainstream display utilized as a role of big business frameworks; be that as it may, this model has extreme security issues when connected to cloud frameworks. An exemplary RBAC display utilizes reference screens running on information servers to execute approval. Be that as it may, the servers in the cloud are out of the control of big business spaces and, subsequently, must be thought about untrusted as a matter of course. Subsequently,

building a powerful information insurance component for cloud-based endeavour frameworks has turned into a noteworthy test. As delicate information might be put away in the cloud for sharing reason or advantageous access; and qualified clients may likewise get to the cloud framework for different applications and administrations, client confirmation has turned into a basic role for any cloud framework. In most existing plans, the span of ciphertext directly develops with the quantity of properties engaged with the entrance strategy, which may acquire an expansive correspondence overhead and calculation cost. This will confine the utilization of asset obliged clients. The characteristic level denial is extremely troublesome since each trait is possibly shared by various clients. The proposed plot gives two-factor security system to improve the secrecy of outsourced information. RNS calculation will be used for the encryption and decoding process included and which guarantees the framework is quick, most solid and is executed with the slightest computational expenses

2. Literature Survey

The criticality and significance of security perspective in distributed storage framework is dissected in different past reviews. Zechao Liu talked about a dynamic characteristic based access control plan to perform quality renouncement and approach updates and considers numerous trait experts in this plan which can work freely with no collaboration and nearness of any focal specialist. BO LANG proposes an independent assurance system for outsourced venture information. Notwithstanding being good with the current RBAC framework, this strategy additionally enables clients to indicate other required strategies for every datum question. Hui Ma_, Rui Zhang_, Zhiguo Wan proposes a plan where in substantial calculations are outsourced to Encryption Service Providers (ESPs) or Decryption Service Providers (DSPs), leaving just a single roleicular exponentiation computation for the sender or the collector. Jianghong Wei displayed a framework where a focal authority isn't required to issue different traits. Each characteristic authority can autonomously issue important keys for the users. Kaiping Xue exhibited a successful focal expert to create mystery keys for the clients. An examining instrument is proposed to identify which characteristic authority has inaccurately or perniciously performed authenticity confirmation system.

Saraswati Gore1, Ashokkumar Kalal exhibited a study paper clarifying the two factor get to control approach for multi-authority distributed storage frameworks. Jiguo Li, Wei Yao proposed a plan for productive client impact shirking. A CP-ABE conspire with productive characteristic disavowal is proposed. Pranayanath Reddy Anantula1, 2Dr G Manoj Someswar proposed an OTP based two factor verification conspire for multi-authority cloud frameworks. Boyang Wang, Student Member proposed public examiner system for guaranteeing two factor cloud security.

3. Existing System

Multi-authority attribute-based systems are either unreliable in quality level disavowal or absence of productivity in correspondence overhead and

calculation cost. RSA calculation is generally utilized for the encryption and unscrambling Encryption in view of bit esteem and henceforth slower contrasted with decimal esteem based encryption In most existing plans, the extent of ciphertext directly develops with the quantity of properties associated with the entrance arrangement, which may bring about a substantial correspondence overhead and calculation cost. This will confine the use of asset obliged clients. More inclined to security assaults as the regularly utilized encryption strategies included does not bolster split offers of information

4. Proposed System

The proposed framework gives two-factor assurance instrument to upgrade the secrecy and approval to the outsourced information on cloud servers.

• Attribute-based access control arrangement guarantees that the end client will be approved by means of a credit mystery key to the information on cloud server.

• The RNS calculation encodes the delicate information in the cloud

The architecture of proposed system is shown in figure 1.

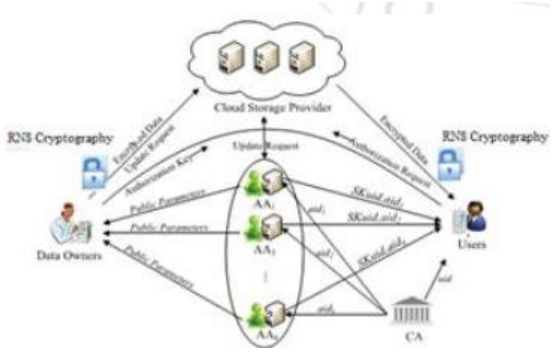

Figure 1: Architecture of Proposed System

The Attribute-based access results in a steady size figure content unscrambling and lessen the correspondence overhead and calculation cost of the framework. RNS calculation utilized for the encryption and decoding advances execution as the number juggling includes decimal estimation of byte and can be prepared in parallel by role the encoded information. The arrangement bolsters characteristic level renouncement and information proprietor/directors can perform client level disavowal.

The framework of the proposed scheme consists of the following phases:

A. Phase 1: System Initialization: First, the CA creates some worldwide public parameters for the framework, and acknowledges both the AA enlistment and client enrolment. At that point, every AA and information proprietor individually produces people in general parameters and mystery data utilized all through the execution of framework.

B. Phase 2: Secret Key and Authorization Generation: When a client presents a demand of credit enlistment to AA, the AA appropriates the relating characteristic mystery keysto this client if his/her authentication is genuine utilizing RNS encryption. At the point when a client presents an approval demand to information proprietor, the information proprietor produces the relating approval key and conveys it to this client.

C. Phase 3: Data Encryption: For each common information, the information proprietor initially characterizes an entrance arrangement, and after that scrambles the information under this predetermined access strategy. From that point, the information proprietor outsources this ciphertext to the CSP. The encryption operation

will utilize an arrangement of public keys from the included AAs and the information proprietor's approval mystery key utilizing RNS encryption.

D. Phase 3: Data Decryption: All the clients in the framework are permitted to question and download any intrigued figure writings from the CSP. A client can recoup the outsourced information, just if this client holds the adequate trait mystery keys as for get to approach and approval key concerning outsourced information utilizing RNS encryption.

E. Phase 5: User-level Revocation: keeping in mind the end goal to disavow a client's entrance benefit, the information proprietor creates another approval mystery key utilized for approval, an arrangement of approval refresh keys for non-denied clients and an arrangement of figure content refresh roles for figure content refresh. While accepting the approval refresh key, each non-disavowed client refreshes the approval key and acquires the new form. All the included figure writings will be refreshed by the CSP in view of the arrangement of figure content refresh segments.

5. Algorithm

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

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, execution examinations and trial comes about show that the proposed conspire is reasonable to information get to control for multi expert distributed storage frameworks.

7. Conclusion

Cloud is being utilized broadly and it will be utilized significantly more lately on which will prompt more stockpiling and sharing of delicate information by means of cloud. This calls for enhanced cloud server security and information level security. The proposed arrangement address the requirement for enhanced cloud server security and information level security by utilizing an Attribute-based access control plot with two-factor insurance alongside the RNS calculation to take it the following level. Security ought to be constant change and should be.

References

[01] N. Jain, D. Kit, P. Mahajan, P. Yalagandula, M. Dahlin, and Y. Zhang, “Star: Self-tuning

aggregation for scalable monitoring," in VLDB, 2007.

[02] J. Liang, X. Gu, and K. Nahrstedt, "Self-configuring information management for large-scale service overlays," in INFOCOM, 2007.

[03] Y. Zhao, Y. Tan, Z. Gong, X. Gu, and M. Wamboldt, "Self-correlating predictive information tracking for large-scale production systems," in ICAC, 2009.

[04] D. Moldovan, G. Copil, H.-L. Truong, and S. Dustdar, "Mela: Monitoring and analyzing elasticity of cloud services," in CloudCom. IEEE, 2013.

[05] Amazon. Aws security center. http://aws.amazon.com/security/. Accessed Nov. 5, 2016.

[06] PublicStack. PublicStack Keystone. http://docs.publicstack.org/developer/keystone/. Accessed Nov. 5, 2016.

[07] PublicStack Neutron. https://wiki.publicstack.org/wiki/Neutron. Accessed Nov. 5, 2016.

[08] L. Huang, M. I. Jordan, A. Joseph, M. Garofalakis, and N. Taft, "Innetwork pca and anomaly detection," in NIPS, 2006.

[09] 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

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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

[15] BO LANG, (Member, IEEE), JINMIAO WANG, AND YANXI LIU, "Achieving Flexible and Self-Contained Data Privacyin Cloud Computing," IEEE Access Journal., date of publication February 7, 2017.

ABOUT AUTHORS:

M.VijayaLakshmi is currently working as an Assistant Professor in Computer Science and Engineering Department, St.Martin's Engineering College, Hyderabad. Her research includes networking and data mining. D.Navanitha is

currently working as an Assistant Professor in Computer Science and Engineering Department, St.Martin's Engineering College, Hyderabad. Her research includes networking and data mining.