International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 4 | ISSN : 2456-3307

Efficient Access Control for Security of Cloud Storage Systems Using RNS Cryptography

B. NVSK Gayathri[1], G. Rajendra[2]

[1]Student, Department of MCA, , Lakireddy Balireddy Engineering College, Mylavaram, Andhra Pradesh, India

[2]Associate Prof, Department of MCA, , Lakireddy Balireddy Engineering College, Mylavaram, Andhra Pradesh, India

ABSTRACT

Developing highlights of the distributed storage administrations empowers information proprietors to store their huge information in the cloud and give the information access to the clients. As protection and security of the cloud server isn't guaranteed, an Attribute-Based Encryption (ABE) a promising strategy for information get to control in distributed storage is used in this undertaking. Trait based encryption, particularly for cipher text arrangement quality based encryption, can satisfy the usefulness of fine-grained get to control in distributed storage frameworks. In the proposed conspire, any client can recuperate the outsourced information if and just if this client holds adequate trait mystery keys as for the entrance strategy and approval enter as to the outsourced information. Both the extent of cipher text and the quantity of matching tasks in decoding are consistent, which diminish the communication overhead and algorithm cost of the framework. Residue Number Systems (RNS) are valuable for dispersing vast dynamic range algorithms over little measured rings, which permits the accelerate of algorithms. RNS algorithm will be utilized for the encryption and unscrambling process included, which can be utilized to accomplish performance change as the number-crunching includes littler numbers and should be possible in parallel. This guarantees the framework is quick, most solid and is executed with the minimum computational expenses.

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

I. INTRODUCTION

The present day multi-authority property based cloud frameworks are either unreliable in quality level repudiation or absence of proficiency in communication overhead and algorithm cost. As the cloud servers can't be completely trusted and may endeavour to get to client information for illicit reason, the worry about information security and protection emerges. One basic strategy for lightening this issue is to store information in scrambled shape, which is more imperative for ensuring touchy client information. In any case, this delivers new difficulties: how to acknowledge get to control over scrambled information that is, sharing classified information on cloud servers [1], [10]. Presently, role based access control (RBAC) display is the most prevalent model utilized as a part of big business frameworks; be that as it may, this model has serious security issues when connected to cloud frameworks. An exemplary RBAC demonstrate 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 locations and, along these lines, must be thought about untrusted of course. Thus, fabricating a successful information security component for cloud-based endeavor frameworks has turned into a noteworthy test [2], [10]. 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 segment for any cloud framework [3].

In most existing plans, the measure of ciphertext directly develops with the quantity of traits engaged with the entrance strategy [10], which may cause an expansive communication overhead and algorithm cost. This will restrain the utilization of resource obliged clients. The characteristic level repudiation is exceptionally troublesome since each quality is possibly shared by numerous clients. The proposed plot gives two-factor security component to improve the secrecy of outsourced information. RNS algorithm will be used for the encryption and decoding process included and which guarantees the framework is quick, most dependable and is executed with the minimum computational expenses

II. LITERATURE SURVEY

The criticality and significance of security angle in distributed storage framework is examined in different past reviews. Zechao Liu [1] talked about a dynamic trait based access control plan to perform property denial and arrangement updates and considers various quality experts in this plan which can work freely with no participation and nearness of any focal specialist. BO LANG [2]proposes an independent insurance instrument for outsourced venture information. Notwithstanding being perfect with the current RBAC framework, this technique additionally enables clients to determine other required approaches for every datum question. Hui Ma, Rui Zhang, Zhiguo Wan [3] proposes a plan where in substantial algorithms are outsourced to Encryption Service Providers (ESPs) or Decryption Service Providers (DSPs), leaving just a single secluded exponentiation algorithm for the sender or the beneficiary. Jianghong Wei[4] displayed a framework where a focal expert isn't required to issue different properties. Each trait specialist can freely issue significant keys for the users.KaipingXue [5] introduced a powerful focal expert to create mystery keys for the clients. An examining instrument is proposed to distinguish which quality specialist has inaccurately or vindictively performed authenticity check method.

Saraswati Gore1, Ashokkumar Kalal2[6] exhibited an overview paper clarifying the two factor get to control approach for multi-expert distributed storage frameworks. Jiguo Li, Wei Yao [7] proposed a plan for proficient client impact shirking. A CP-ABE plot with productive quality disavowal is proposed. Pranayanath Reddy Anantula1, 2Dr G Manoj Someswar [8] proposed an OTP based two factor validation conspire for multi-authority cloud systems.Boyang Wang, Student Member [10] proposed open evaluator instrument for guaranteeing two factor cloud security.

III. EXISTING SYSTEM

Multi-authority quality based frameworks are either unreliable in characteristic level disavowal or absence of proficiency in communication overhead and algorithm cost.RSA algorithm is generally utilized for the encryption and decryption. Encryption in light of bit esteem and consequently slower contrasted with decimal esteem based encryption. In most existing plans, the measure of ciphertext straight develops with the quantity of properties associated with the entrance approach, which may bring about an expansive communication overhead and algorithm cost. This will restrain the use of resource compelled clients. More inclined to security assaults as the ordinarily utilized encryption methods included does not support split offers of information.

IV. PROPOSED SYSTEM

The proposed framework gives two-factor assurance system 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 an ascribe mystery key information on cloud server.
• The RNS algorithm encodes the touchy information in the cloud

The engineering of proposed framework is appeared in figure 1.

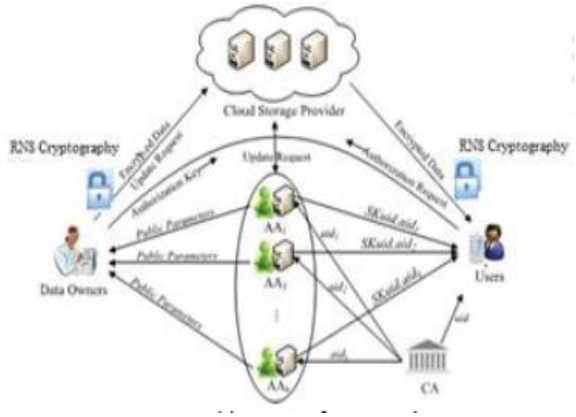

Figure 1. Architecture of Proposed System

The Attribute-based access brings about a steady size cipher text decoding and lessens the communication overhead and algorithm cost of the framework. RNS algorithm utilized for the encryption and decoding upgrades performance as the number juggling includes decimal estimation of byte and can be handled in parallel by part the scrambled information. The arrangement bolsters quality level repudiation and information proprietor/managers can perform client level disavowal. The structure of the proposed plot comprises of the accompanying stages:

System Initialization: To begin with, the CA produces some worldwide open parameters for the framework, and acknowledges both the AA enrolment and client enlistment. At that point, every AA and information proprietor individually produce general society parameters and mystery data utilized all through the performance of framework.

Secret Key and Authorization Generation: At the point when a client presents a demand of trait enlistment toAA, the AA circulates the relating characteristic mystery keys to this client if his/her authentication is trueusing RNS encryption. At the point when a client submits anauthorization demand to information proprietor, the information proprietor generates the relating approval key and conveys it to this client.

Data Encryption: For each mutual information, the information proprietor initially characterizes an accesspolicy, and after that encodes the information under this predetermined accesspolicy. From there on, the information proprietor outsources this ciphertextto the CSP. The encryption activity will utilize an arrangement of publickeys from the included AAs and the information proprietor's authorizationsecret keyusing RNS encryption.

Data Decryption: Every one of 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 thesufficient quality mystery keys as for get to policy and approval key with respect to outsourced information utilizing RNS encryption.

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-renounced clients and an arrangement of cipher text refresh parts for cipher text refresh. While getting 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 cipher text refresh segments.

V. ALGORITHM

In this project we have utilized RNS (Residue number framework) 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 to be specific Residue Number System algorithm. By utilizing this algorithm the encryption and decoding forms occurred on the given cloud information stockpiling.

VI. RESULTS AND DISCUSSION

Broad security examination, performance correlations and test comes about show that the proposed conspire is reasonable to information get to control for multi specialist distributed storage frameworks.

VII. CONCLUSION

Cloud is being utilized generally and it will be utilized much more later on which prompt more stockpiling and sharing of touchy information by means of will 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 algorithm to take it the following level. Security ought to be ceaseless change and should be.

VIII. REFERENCES

[1]. Jiguo Li, Wei Yao, Jinguang Han, Member, IEEE, Yichen Zhang, and JianShen, "User Collusion Avoidance CP-ABE With Efficient Attribute Revocation for Cloud Storage", IEEE SYSTEMS JOURNAL, 2017.

[2]. 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.

[3]. 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.

[4]. 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.

[5]. W. Lou ,K. Ren,C. Wang and S. Yu (2010) "Achieving secure, scalable, and fine-grained data access control in cloud computing," in INFOCOM'10, IEEE, vol. 4, no. 9, pp. 534–542. 6Guojun Wang, Jie Wu and Qin Liu (2010) "Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services", vol. 11, no. 6,pp. 113–156.

[6]. ShashankAgrawal, ShwetaAgrawal, SaikrishnaBadrinarayanan(2009) "On the Practical Security of Inner Product Functional Encryption", vol. 14, no. 9, pp. 241–310.

[7]. AmitSahai ,Allison Lewko and Tatsuaki Okamoto (2009) "Fully Secure Functional Encryption: AttributeBased Encryption and Hierarchical Inner Product Encryption", vol. 8, no. 21,pp. 564–642.

[8]. A. Beimel(2009) "Secure schemes for secret sharing and key distribution" DSc dissertation, vol. 16, no. 21,pp. 794–948.

[9]. Ferraiolo DF and Kuhun DR. 1992. Role Based Access Control. Proceeding of 15th National Computer Security Conference, Baltimore MD. pp. 554-563.

[10]. R. Lehtinen, D. Russell and G. Gangemi Sr. 2006. Computer Security Basics. O Reilly publications, 2nd edition.
[11]. M. Blaze and J Feigenbaum et al. The Keynote trust management system. Version 2, IETF RFC 270.
[12]. Zechao Liu , Zoe L. Jiang , Xuan Wang, S.M. Yiu§, ChunkaiZhang andXiaomeng Zhao, Fellow, IEEE, "Dynamic Attribute-Based Access Control in Cloud Storage Systems", 2016 IEEE TrustCom/BigDataSE/ISPA
[13]. 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.
[14]. 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.
[15]. Jianghong Wei, Wenfen Liu, and Xuexian Hu "Secure and Efficient Attribute-Based Access Control for Multiauthority Cloud Storagein" IEEE SYSTEMS JOURNAL,2016.
[16]. KaipingXue, Senior Member, IEEE, YingjieXue, 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.
[17]. 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.

ABOUT AUTHORS:

B. NVSK.Gayathri is currently pursuing her MCA in Master Of Computer Applications Department, Lakireddy Balireddy Engineering College, Mylavaram, A.P. She Received her Bachelor Science from ANU university.

G.Rajendra is currently working as an Associate Professor in Master Of Computer Applications Department, Lakireddy Balireddy Engineering College, Mylavaram. His research includes networking and data mining.