ISSN 2320-9984
9 772320 998053 04

Volume 5 Issue 4| December 2017 ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research

Website: www.ijmemr.org

Dynamic Key Generation Based Data Retrieval In Cloud Environment

Shweta Singh Rajput
M.Tech. Research Scholar
Branch Cyber Security
Oriental Institute of Science and Technology
Bhopal (M.P.), [INDIA]
Email: ssr19dec@gmail.com

Sanjay Sharma
Assistant Professor
Department of Computer Science & Engineering
Oriental Institute of Science and Technology
Bhopal (M.P.), [INDIA]
Email: sanjaysharma@oriental.ac.in

***Abstract*—*The data retrieval of cloud based services faced a problem of authentication and authorization of user. The cloud environments provide the dynamic data updating in cloud storage. For the authentication of user cloud provides the key generation process based on different cryptography algorithms. The cryptography algorithms generate the session key for the authorization of user. In this paper proposed the dynamic key based user authentication and authorization process. The generation of key provides two types of files one is fake file and other is original file. If the illegal user hits the cloud server, the cloud server provides the fake file. The proposed model implemented in JAVA and RMI control. For data storage used MYSQL.*

***Keywords:*—*Cloud storage, Dynamic key, TPA, Security*

1. INTRODUCTION

Cloud data storage and access of data faced a big security issue in concern of security and validation of user authentication [4]. For the authentication of user used various cloud security model. All cloud security model used cryptography technique for the generation of key for access of data and retrieval of data. The data dynamics process provides the ownership of data to the user. User modified the process of data such as insertion, deletion and modification over the cloud network [2-3]. The process of data dynamics precedes along with cryptography and third-party auditor. The third -party auditor provides the access link between cloud service provider and users. The processing of cloud computing infrastructure involved three parties for the processing of data storage and data retrieval. Cloud Computing is not just a third-party data warehouse [6-9]. The data stored in the cloud may be frequently updated by the users, including insertion, deleting, modification, appending, reordering, etc[1]. To ensure storage correctness under dynamic data update is hence of paramount importance. However, this dynamic feature also makes traditional integrity insurance techniques futile and entails new solutions. Last but not the least, the deployment of Cloud Computing is powered by data centers running in a simultaneous, cooperated and distributed manner. Individual user's data is redundantly stored in multiple physical locations to further reduce the data integrity threats [1,5]. Therefore, distributed protocols for storage correctness assurance will be of most importance in achieving a robust and secure cloud data storage system in the real world. The current decade ensures the remote data integrity over the cloud network for the processing of public cloud. These techniques, while can be useful to ensure the storage correctness without having users possessing data, cannot address all the security

threats in cloud data storage, since they are all focusing on single server scenario and most of them do not consider dynamic data operations [10-12]. In cloud data storage, a user stores his data through a CSP into a set of cloud servers, which are running in a simultaneous, cooperated and distributed manner. Data redundancy can be employed with technique of erasure-correcting code to further tolerate faults or server crash as user's data grows in size and importance. Thereafter, for application purposes, the user interacts with the cloud servers via CSP to access or retrieve his data. In some cases, the user may need to perform block level operations on his data [20]. In section 3 discuss proposed Work. In section 4 discuss the experimental result and analysis. finally discuss conclusion & future work in section 5.

2. KEY GENERATION PROCESS

Here discusses the dynamic key generate which is the main contribution in our proposed in addition to the type of confidential information shared between the user and server [18]. Our scheme requires two set of keys to be generated at each party's side: secondary keys (Ki)s and session key (SK)s. (Ki)s are necessary to generate V values, which are used as a security enhancement step to generate session keys. The node N1 will issue the intermediate node (IN) and a data stored over cloud [13-16].

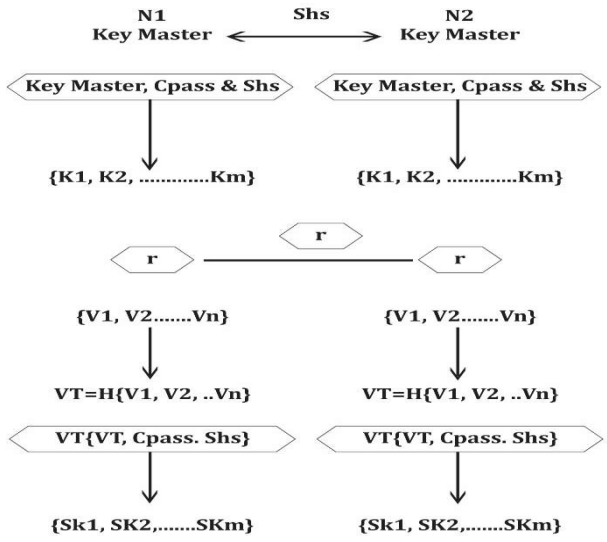

Figure 1: Shows key generation technique [17].

3. PROPOSED METHODS AND MODEL

The cloud storage and data encryption process in user and TPA. The user used the process of key generation and file encryption process using cyclic shift key technique. the encrypted file verifies by the TPA. If the content of file is edited by TPA and some other one the file cannot be uploaded over cloud server. The algorithm description given below:

a. 1 .

KEY GENERATION PROCESS

(a) Input user data D
(b) The cyclic key process creates to key value Uk and TK
(c) UK key used for client and Tk key used by TPA
(d) Uk key pass the value of file and encrypted the user data with bit operation.

2. TPA VERIFICATION

(a) TPA receive the Key of Tk of user file
(b) TPA verify the user status and conform the value of Key
(c) If value of key is not matched then file cannot be uploaded.

3. PROOF OF RETRIEVAL

(a) If user download the file TPA send the Uk key
(b) The value of Uk=TK then file is download
(c) If file is edited the size of Uk is changed then edited file cannot be uploaded

MODEL DESCRIPTION

The processing of model describes in five phases for the process of data.

1. User Registration section
2. cloud storage section
3. privilege of data access
4. privilege of data download
5. cloud server data verification

The below figure shows Security Model for Data Storage which contain three entities and the operation occurred between them. Then, let we discuss the phase mentioned above in detail.

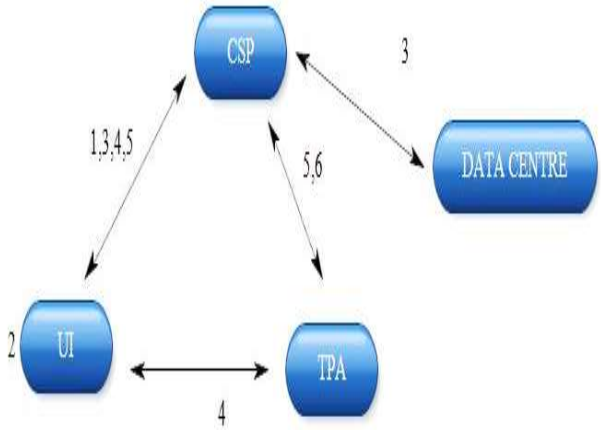

Figure 2: Security Model for over cloud.

4. EXPERIMENTAL RESULT ANALYSIS

Here discusses the dynamic key generate which is the main contribution in our proposed in addition to the type of confidential information shared between the user and server. Our scheme requires two set of keys to be generated at each party's side: secondary keys (Ki)s and session key (SK)s. (Ki)s are necessary to generate V values, which are used as a security enhancement step to generate session keys. The node N1 will issue the intermediate node (IN) and a data stored over cloud.

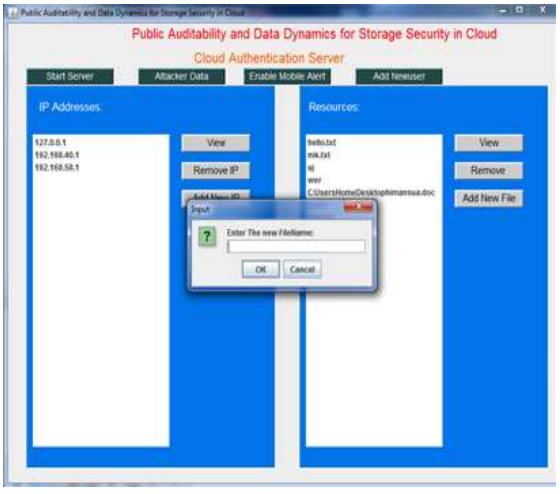

Figure 3: Window show that the click on owner file modification in our cloud data storage based on key authentication implementation.

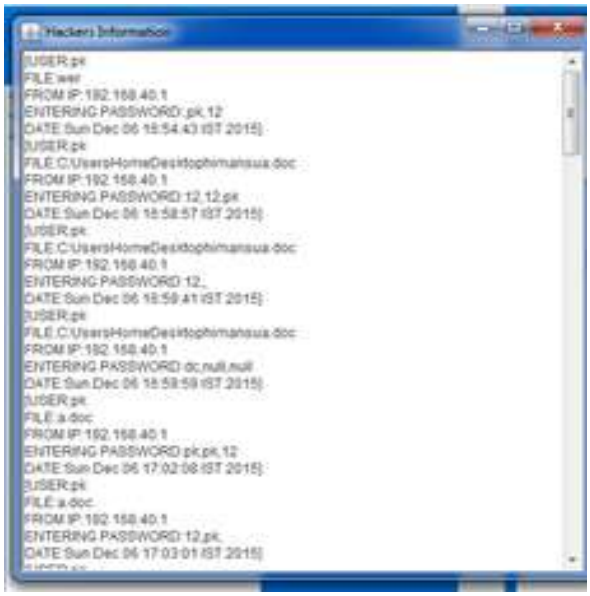

Figure 4: window show that the log file of users in all mode illegal and normal users.

Table 1: The comparative performance for original and fake files based on number of hit and miss ratio in percentage value for the Solid and Gas file.

Types of File	File Name	Correct Key in %	Incorrect Key in %
Original File	**Solid.txt**	0.88	0.12
Fake file	**Gas.txt**	0.81	0.19

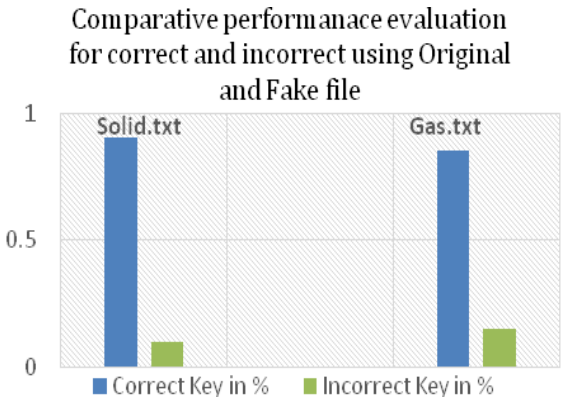

Figure 5: The comparative performance evaluation graph for original and fake files based on number of correct and incorrect in percentage value for the Solid and Gas file.

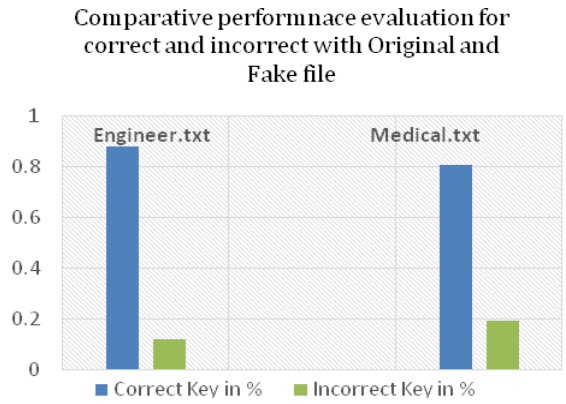

Figure 6: The comparative performance evaluation graph for original and fake files based on number of correct and incorrect in percentage value for the engineer and medical file.

Table 2: The comparative performance for Computation time on the basis of data size using methods RSA and Proposed with text. file.

Data size-text. file	RSA Method	Proposed Method
3	185	170
5	195	180
7	205	190
9	215	200
11	225	210
13	235	220
15	245	230
17	255	240
19	265	250
21	275	260

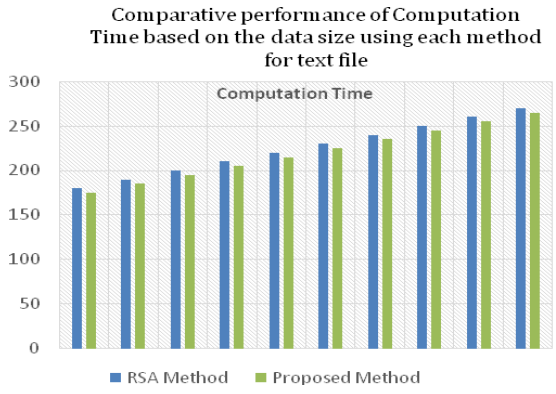

Figure 7: The comparative performance for Computation time on the basis of data size using each method like, RSA and Proposed with text file, here we find the value of computation time for respectively data size and methods.

5. CONCLUSION AND FUTURE WORK

It is evidently critical situation within the cloud cannot be over emphasized due to threats from within and outside of the cloud environments. Privacy and data Security responsibilities within the cloud should be a collaborative effort between both service providers and users. These responsibilities differ by the kind of cloud services been consumed. The cloud service provides is on duty to ensure the security of cloud data storage and to ensure maximum protection. Service providers have the responsibility to ensure the public data integrity and isolation protections are put in place to mitigate the risks users pose to one another in terms of data loss, misuse, or privacy violation within the cloud. Again, from the cloud service provider's perspective, there should be an active monitoring mechanism in place to allow for effective planning and implementation of services. This also serves as a means to respond to events quickly and more efficiently. Cloud users on the other hand must ask and be clear about their responsibility for their security.

REFERENCES:

[1] Jin Li, Xiao Tan, Xiaofeng Chen, Duncan S. Wong, Fatos Xhafa, "OPOR: Enabling Proof of Retrievability in Cloud Computing with Resource-Constrained Devices" IEEE 2015, Pp 195 205

[2] Qian Wang, KuiRen, Member, Wenjing Lou, Jin "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing" IEEE 2011 847 -859

[3] Meera Chheda, Anmol Achhra, Priyanka Vaswani, Rajeshwari Agale, Vidya Bhise. "Public Auditing for The Shared Data in The Cloud". International Journal of Advance Foundation and Research in Computer (IJAFRC) 2015 Pp 724-728.

[4] Prof. N.L. Chourasiya, Dayanand Lature, Arun Kumavat, Vipul Kalaskar, Sanket Thaware. "Privacy-Preserving Public Auditing for Secure Cloud Storage" International Journal of Engineering Research and General Science, 2015Pp 744 -748.

[5] R. Guruprasath, M. Arulprakash "Privacy Preserving Public Auditing For Shared Data with Large Groups in The Cloud" Journal of Recent Research in Engineering and Technology 2015 Pp 40-46

[6] Mrunali Pingale, Prof. Jyoti Pingalkar "Security Preserving Access Control Mechanism In Public Clouds Using PANDA Security Mechanism" iPGCON, 2015 Pp 1-5.

[7] Pradnya Chikhale, Namrata Dwivedi, Parna Dutta, Aparajita Sain, Vrunda Bhusari "Enhancing Data Storage Security in Cloud Computing Using PDDS Technique" PISER 2014 Pp 53 -59.

[8] J. Aparna, Mr. R.Sathiyaraj "Auditing Mechanisms for Outsourced Cloud Storage" International Journal of Computer Science and Mobile Computing, 2014, Pp 219-229

[9] Ch. Rajeshwari, S. Suresh "An Efficient PDP Scheme for Distributed Cloud Storage to Support Dynamic Scalability on Multiple Storage Servers" International Journal of Science Engineering and Advance Technology, 2014 Pp 985-988

[10] Betzy K. Thomas, M. Newlin Rajkumar "A Dynamic Public Auditing Security Scheme To Preserve Privacy in Cloud Storage" IJSHJE 2013 Pp 93-97.

[11] Guangyang Yang, Hui Xia, Wenting Shen, XiuxiuJiang, Jia Yu "Public Data Auditing with Constrained Auditing Number for Cloud Storage" 2015 IJSIA Pp 21-32.

[12] Jian Yang, Haihang Wang, Jian Wang, Chengxiang Tan, Dingguo "Provable Data Possession of Resource-constrained Mobile Devices in Cloud Computing" Journal of Networks, 2011 pp1033-1040.

[13] Javed Akthar Khan, Ritika Arora "A Review of Cloud Environment and Recognition of Highly Secure Public Data Verification Architecture using Secure Public Verifier Auditor" International Journal of Electrical, Electronics and Computer Engineering 2014 pp144-148.

[14] Harleen Kaur, Er. Vinay Gautam "A Survey of Various Cloud Simulators" International Journal of Computer Sciences and Engineering, 2014 Pp35 - 38.

[15] Clementine Gritti, Willy Susilo, Thomas Plantard, Rongmao Chen "Improvements on Efficient Dynamic Provable Data Possession scheme with Public Veriability and Data Privacy" Centre for Computer and Information Security Research 2014 pp 1-19.

[16] Chunming Gao, Noriyuki Iwane "A Social Network Model with Privacy Preserving and Reliability Assurance and Its Applications in Health Care" International Journal of Energy, Information and Communications 2015, pp.45-58.

[17] Mohammad Iftekhar Husain Steve Ko Atri Rudra Steve Uurtamo "Almost Universal Hash Families Are Also Storage Enforcing" Department Of Computer Science And Engineering, University At Buffalo 2012 Pp 1-18.

[18] Chintal Maisheri, Deepak Sharma" Enabling Indirect Mutual Trust for

Cloud Storage Systems". International Journal of Computer Applications 2013 Pp 1-11

[19] Frank Hans-Ulrich Doelitzscher "Security Audit Compliance for Cloud Computing" Plymouth University, Thesis 2014

[20] B. Krishna Kumari, S. Swapna "Stability Based Service for Secure Cloud Storage" IJITECH, 2015 Pp0399-0403.