iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** III **Month of publication:** March 2019

DOI: http://doi.org/10.22214/ijraset.2019.3448

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

An Efficient Auditing Protocol for Information Sharing and Secured Distributed Storage

Rachana. R[1], Shanthi.S[2], Mrs.A.Shanthakumari[3]
[1]*M.E., Associate professor,* Department of Computer Science and Engineering, Prince Dr K Vasudevan Engineering College, Ponmar, Chennai, India

***Abstract*: Data sharing can be achieved with sensitive information hiding in remote data integrity auditing, and propose a new concept called identity based shared data integrity auditing with sensitive information hiding for secure cloud storage. Initially every data would be outsourced to the cloud only after authorized or activated by the proxy. The key would be generated to the file randomly by the key generation center. The transaction details such as key mismatch, file upload and download, hacking details would be shown to the proxy and cloud server. The automatically file would be recovered by the user even if hacker access or tamper the file. The main motive is to ensure that when the cloud properly stores the users sanitized data, the proof it generates can pass the verification of the third party auditor.**

Keywords: Cloud audit, recovery of file, information hiding.

I. INTRODUCTION

In Information security is the process of securing information data from unauthorized aceesses. With the increased use of electronics media in our personal lives as well as businesses, the possibility of security breach and its major impact has increased. The theft of personal identity, credit card information, and other important data using hacked user names and passwords have become common these days. In addition, the theft of confidential business data may lead to loss of business for commercial organizations. Remote data integrity auditing schemes, the data owner firstly needs to generate signatures for data blocks before uploading them to the cloud. These signatures are used to prove the cloud truly possesses these data blocks in the phase of integrity auditing. And then the data owner uploads these data blocks along with their corresponding signatures to the cloud. A potential method of solving this problem is to encrypt the whole shared file before sending it to the cloud, and then generate the signatures used to verify the integrity of this encrypted file, finally upload this encrypted file and its corresponding signatures to the cloud. This method can realize the sensitive information hiding since only the data owner can decrypt this file. The word is used in information technology, including: network forensics the capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents. The word forensics refers to used for formal public debate or discussion.

Centre for education and research Information Assurance and Security (CERIAS) is a center for research and education in areas of information security that are crucial to the protection of critical computing and communication infrastructure. Key exposure is one serious security problem for cloud storage auditing. A vulnerability is a weakness in design, implementation, operation or internal control. Most of the vulnerabilities that have been discovered are documented in the Common Vulnerabilities and Exposures (CVE) database.

In existing system more organizations and individuals would like to store their data in the cloud. However, the data stored in the cloud might be corrupted or lost due to the inevitable software bugs, hardware faults and human errors in the cloud. The sensitive information should not be exposed to others when the cloud file is shared. Encrypting the whole shared file can realize the sensitive information hiding, but will make this shared file unable to be used by others. If the file has been hacked by hacker it only recovers the file.

The main disadvantages in the existing system are the cloud and the shared users are untrustworthy, all of the sensitive information of the file will not be exposed to them. The explosive growth of data, it is a heavy burden for users to store the sheer amount of data locally. Remote data integrity auditing schemes cannot support data sharing with sensitive information hiding.

A cryptosystem or an algorithm, is any secret method of bypassing normal authentication or security control that may exist for a number of reasons, including by original design or from poor configuration. Attackers can deny service to individual victims. These are all provided security by an information security. There are many algorithms used to provide security by an every stage of proxy systems.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

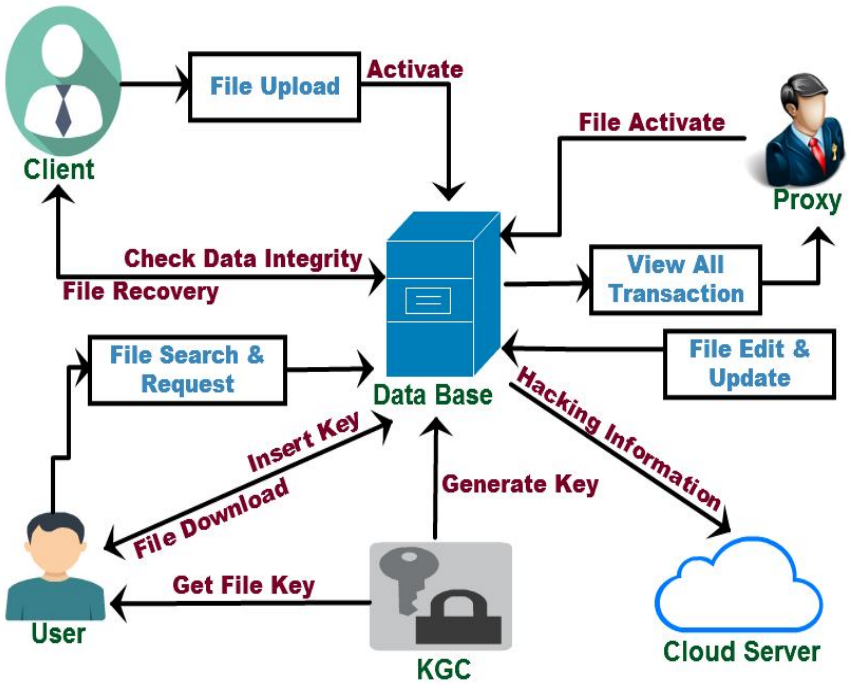
II. PROPOSED SYSTEM

Remote data integrity auditing is future to guarantee the integrity of the data stored in the cloud. In some common cloud storage systems such as the Electronic Health Records system, the cloud file strength contains some sensitive information. We explore how to achieve data sharing with sensitive information hiding in identity-based integrity auditing for secure cloud storage. A sanitizer is used to sanitize the data blocks corresponding to the sensitive information of the file and transforms these data blocks' signatures into valid ones for the sanitized file. These signatures are used to verify the integrity of the sanitized file in the phase of integrity auditing. As a result, our scheme makes the file stored in the cloud able to be shared and used by others on the condition that the sensitive information is hidden, while the remote data integrity auditing is still able to be efficiently executed.

The main advantages are to investigate how to achieve data sharing with sensitive information hiding in remote data integrity auditing, and propose a new concept called identity-based shared data integrity auditing with sensitive information hiding for secure cloud storage. The sanitizer can be viewed as the administrator of the information system in a hospital. The personal sensitive information should not be exposed to the sanitizer. To preserve the privacy of patient from the sanitizer, the medical doctor will blind the patient's sensitive information of each record before sending this record to the sanitizer. The medical doctor then generates signatures for this blinded record and sends them to the sanitizer. The sanitizer stores these messages into record information analyst.

III. SYSTEM ARCHITECTURE

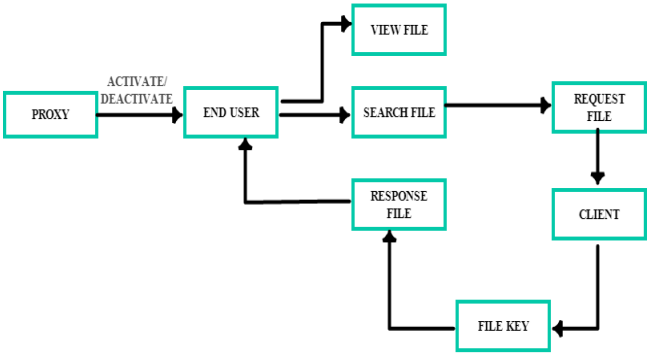
Design Engineering deals with the various diagrams for the implementation of project. Design is the creation of a plan or convention for the construction of an object, system or measurable human interaction such as in architectural blueprints, engineering drawings, business process, circuit diagrams and sewing patterns. Design has different connotations in different fields. Software design is a process through which the requirements are translated into representation of the model. The UML offers a way to visualize a system's architectural blueprints in a diagram. UML provides a comprehensive notation for the full life cycle of object oriented design documentation, the UML has been extended to cover a larger set of design documentation, and been found useful in many contexts. System design contains logical design and physical Design, Logical Designing describes the structures& characteristics or features, like input, output, files, database & procedures. Thus designing a system architecture it protects from explaining a detailed design and it provides a security among all the details within a system process which provides a overall detail among the structure within a system.



International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

IV. FLOWDIAGRAMS

The Flow diagram are used to represent the flow of diagrams that can be managed and provided a security among each and every process that can accessed only with the help of proxy. These flow diagrams can process and accessed with the modeled flow of data. The data flow set of diagrams activates and deactivates the process which will be governed each by proxy. These set of proxy development with the activation or deactivation of each and every set of details within the requested or response file of an data processes.



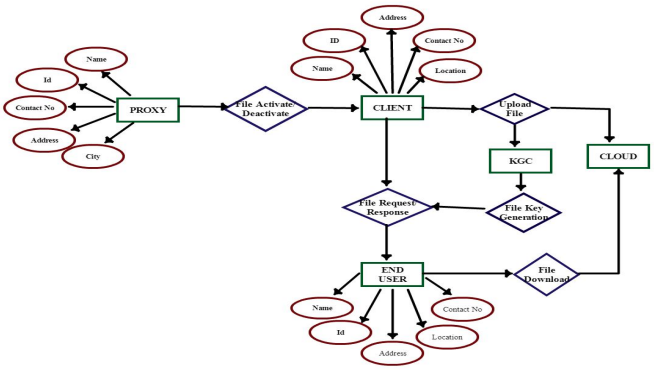
V. DESCRIPTIONS OF MODULES

The data owner firstly needs to generate signatures for data blocks before uploading them to the cloud. These signatures are used to prove the cloud truly possesses these data blocks in the phase of integrity auditing. And then the data owner uploads these data blocks along with their corresponding signatures to the cloud. The data stored in the cloud is often shared across multiple users in many cloud storage applications. The data owner activate the file to check whether the uploaded file is appropriate or not then the Proxy also activate the file to check the file is Good. Data integrity auditing scheme that realizes data sharing with sensitive information hiding. However, the data stored in the cloud might be corrupted or lost. Data integrity auditing on the condition that the sensitive information of shared data is protected.

VI. RESULT

The algorithm used here are Identity-based cryptography which simplifies complex management, security Analysis and achieves desirable security and efficiency, Hierarchial attribute based encryption which based on key generation. The project implement modules as a result of implementing the project are File uploading and activation, Data Integrity Auditing, Sensitive Information Sharing, Generating Key Signature, File Security and Recovery. The data owner firstly needs to generate signatures for data blocks before uploading them to the cloud. The data owner uploads these data blocks along with their corresponding signatures to the cloud. The data stored in the cloud is often shared across multiple users in many cloud storage applications. The data owner activate the file to check whether the uploaded file is appropriate or not. The Proxy also activate the file to check the file is Good.

The rapid development of cloud storage services makes it easier than ever for cloud users to share data with each other. To ensure users' confidence of the integrity of their shared data on cloud, a number of techniques have been proposed for data integrity auditing with focuses on various practical features. The secure KNN algorithm is to encrypt index and query vectors.



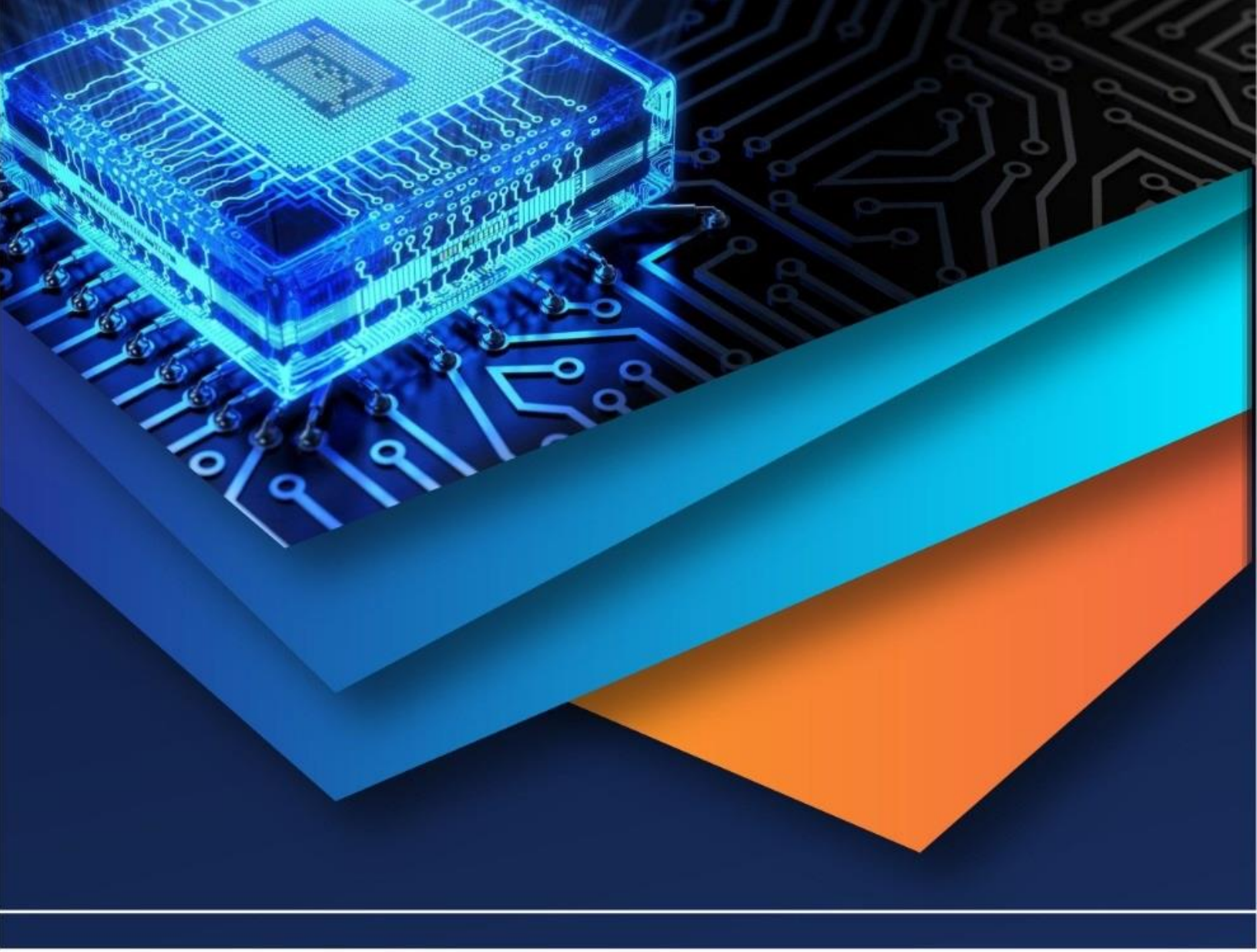
VII. CONCLUSION

Here it proposes a character based information respectability reviewing plan for secure distributed storage, which bolsters information offering to delicate data covering up. In our plan, the record put away in the cloud can be shared and utilized by others depending on the prerequisite that the touchy data of the document is ensured. Moreover, the remote information honesty examining is still ready to be proficiently executed. The security evidence and the exploratory investigation exhibit that the proposed plot accomplishes attractive security and productivity.

In this paper, the data owner independently upload the data to the Cloud and it is difficult to monitor the data and checking the process. This can be achieved by introducing Proxy component to check for the integrity. This is an added advantage to the data owner that he need not stay for integrity checking. The data owner provides a key to the proxy server using that key proxy is responsible for checking the data. This should be considering as the future work to overcome this drawback.

REFERENCES

[1] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, Jan 2012.
[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS '07, 2007, pp. 598–609.
[3] A. Juels and B. S. Kaliski, "Pors: Proofs of retrievability for large files," in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS '07, 2007, pp. 584–597.
[4] H. Shacham and B. Waters, "Compact proofs of retrievability," J. Cryptology, vol. 26, no. 3, pp. 442–483, Jul. 2013.
[5] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," IEEE Transactions on Computers, vol. 62, no. 2, pp. 362–375, 2013.
[6] S. G. Worku, C. Xu, J. Zhao, and X. He, "Secure and efficient privacy-preserving public auditing scheme for cloud storage," Comput. Electr. Eng., vol. 40, no. 5, pp. 1703–1713, Jul. 2014.
[7] C. Guan, K. Ren, F. Zhang, F. Kerschbaum, and J. Yu, "Symmetric-key based proofs of retrievability supporting public verification," in Computer Security – ESORICS 2015. Cham: Springer International Publishing, 2015, pp. 203–223.
[8] W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu, and R. Hao, "Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium," Journal of Network and Computer Applications, vol. 82, pp. 56–64, 2017.
[9] J. Sun and Y. Fang, "Cross-domain data sharing in distributed electronic health record systems," IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 6, pp. 754–764, June 2010.
[10] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proceedings of the 4th international conference on Security and privacy in communication netowrks, 2008, pp. 1–10.
[11] C. Erway, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in ACM Conference on Computer and Communications Security, 2009, pp. 213–222.
[12] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847–859, May 2011.
[13] J. Yu, K. Ren, C. Wang, and V. Varadharajan, "Enabling cloud storage auditing with key-exposure resistance," IEEE Transactions on Information Forensics and Security, vol. 10, no. 6, pp. 1167–1179, 2015.
[14] J. Yu, K. Ren, and C. Wang, "Enabling cloud storage auditing with verifiable outsourcing of key updates," IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1362–1375, June 2016.
[15] J. Yu and H. Wang, "Strong key-exposure resilient auditing for secure cloud storage," IEEE Transactions on Information Forensics and Security, vol. 12, no. 8, pp. 1931–1940, Aug 2017.
[16] J. Yu, R. Hao, H. Xia, H. Zhang, X. Cheng, and F. Kong, "Intrusion-resilient identity-based signatures: Concrete scheme in the standard model and generic construction," Information Sciences, vol. 442-443, pp. 158 – 172, 2018.
[17] B. Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud," in 2012 IEEE Fifth International Conference on Cloud Computing, June 2012, pp. 295–302.
[18] G. Yang, J. Yu, W. Shen, Q. Su, Z. Fu, and R. Hao, "Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability," J. Syst. Softw., vol. 113, no. C, pp. 130–139, Mar. 2016.
[19] A. Fu, S. Yu, Y. Zhang, H. Wang, and C. Huang, "Npp: A new privacy-aware public auditing scheme for cloud data sharing with group users," IEEE Transactions on Big Data, 2017. [Online]. Available: DOI:10.1109/TBDATA.2017.2701347
[20] B. Wang, B. Li, and H. Li, "Panda: Public auditing for shared data with efficient user revocation in the cloud," IEEE Transactions on Services Computing, vol. 8, no. 1, pp. 92–106, Jan.-Feb. 2015.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY