ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

An Efficient Secured Public Auditing Protocol with Novel Dynamic Structure for Cloud Data

Varsha P[1], Bhavani T M[2], Thilagavathy T[3], Aiswarya S[4]

UG Scholars, Department of Computer Science and Engineering, Velammal Institute of Technology, Thiruvallur, Tamil Nadu, India[1,2,3]

Assistant Professor, Department of Computer Science and Engineering, Velammal Institute of Technology, Thiruvallur, Tamil Nadu, India[4]

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: Remote data integrity, Data Sharing, Sensitive Information Hiding, Batch Auditing, Cloud Storage.

I. INTRODUCTION

AN increasing number of organizations outsource their data, applications and business processes to the cloud, empowering them to achieve financial and technical benefits due to on-demand provisioning and pay-per-use pricing. However, organizations are still hesitant to adopt cloud services because of security, privacy, and reliability concerns regarding provisioned cloud services as well as doubts about trustworthiness of their cloud service provider . Cloud service certifications (CSC) are good means to address these concerns by establishing trust, and increasing transparency of the cloud market . Several CSC have evolved, such as CSA STAR or EuroCloud Star Audit. These CSC attempt to assure a high level of security, reliability, and legal compliance, for a validity period of one to three years. However, cloud services are part of an ever-changing environment, resulting from fast technology life cycles and inherent cloud computing (CC) characteristics, like on-demand provisioning and entangled supply chains. Hence, such long validity periods may put in doubt reliability of issued certifications. CSC criteria may no longer be met throughout these periods, for instance, due to configuration changes or major security incidents. Thus, continuous auditing (CA) of certification criteria is required to assure transparent, continuously reliable, and secure cloud services and to establish a trustworthy CSC after the initial certification process is accomplished.

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 . In order to verify whether the data is stored correctly in the cloud, many remote data integrity auditing schemes have been proposed . In 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. It is important to accomplish remote data integrity auditing on the condition that the sensitive information of shared data is protected. 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. However, it will make the whole shared file unable to be used by others.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

Continuous Auditing(Batch Auditing)

Continuous auditing or Batch Auditing is defined as a methodology that enables independent auditors to provide written assurance on a subject matter, using a series of auditors' reports issued virtually simultaneously with, or a short period of time after, the occurrence of events underlying the subject matter . Thus, CA enables auditors to immediately react to changes or events concerning the subject matter and to adjust their auditing reports based on assessment of these changes and events.

The early works of Groomer and Murthy (1989) concerning implementation of embedded audit modules and Vasarhelyi and Halper (1991) regarding usage of monitoring and control layers spawned a research stream of CA. Therefrom, extant literature investigates implementation, transferability, and diffusion of CA in varying domains . Recently, researchers discussed CA of enterprise resource planning systems accounting systems and web services . In the context of CC, research started to propose different approaches to enable third party auditing, for example, methodologies to enable auditors to simultaneously verify integrity of multiple users' data and to assure data location compliance by analyzing audit logs . However, a comprehensive CA architecture, which is able to audit a broad range of CSC criteria and combines various methodologies, is still missing.

RELATED WORK

Paper 1

TITLE: Public Integrity Auditing for Dynamic Data Sharing with Multi-User Modification.

AUTHOR: Jiawei Yuan, Shucheng Yu, Member, IEEE

ABSTRACT:

In past years, the rapid development of cloud storage services makes it easier than ever for cloud users to share data witheach other. To ensure users' confidence of the integrity of their shared data on cloud, a number of techniques have been proposedfor data integrity auditing with focuses on various practical features, e.g., the support of dynamic data, public integrity auditing, low communication/computational audit cost, low storage overhead. However, most of these techniques consider that only the original data owner can modify the shared data, which limits these techniques to client read-only applications. Recently, a few attempts started considering more realistic scenarios by allowing multiple cloud users to modify data with integrity assurance.

Paper 2

TITLE: Identity-Based Data Outsourcing with Comprehensive Auditing in Clouds

AUTHOR: Yujue Wang, Qianhong Wu, Member, IEEE, Bo Qin, Wenchang Shi Robert H. Deng, Fellow, IEEE, Jiankun Hu

ABSTRACT:

Cloud storage system provides facilitative file storage and sharing services for distributed clients. To address integrity, controllable outsourcing and origin auditing concerns on outsourced files, we propose an identity-based data outsourcing (IBDO) scheme equipped with desirable features advantageous over existing proposals in securing outsourced data. First, our IBDO scheme allows a user to authorize dedicated proxies to upload data to the cloud storage server on her behalf, e.g., a company may authorize some employees to upload files to the company's cloud account in a controlled way. The proxies are identified and authorized with their recognizable identities, which eliminates complicated certificate management in usual secure distributed computing systems. Second, our IBDO scheme facilitates comprehensive auditing, i.e., our scheme not only permits regular integrity auditing as in existing schemes for securing outsourced data, but also allows to audit the information on data origin, type and consistence of outsourced files. Security analysis and experimental evaluation indicate that our IBDO scheme provides strong security with desirable efficiency.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

II. PROPOSED SYSTEM

SYSTEM MODEL AND SECURITY MODEL

The system model involves different kind of entities: the cloud, the user, the sanitizer, the Key Generation Controller (KGC), the Proxy, Cloud Server..

(1) Cloud : The cloud provides enormous data storage space to the user. Through the cloud storage service, users can upload their data to the cloud and share their data with others.

(2) User: The user is a member of an organization, which has a large number of files to be stored in the cloud.

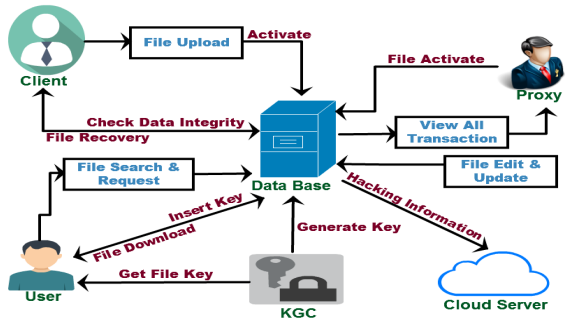
(3) Sanitizer: The sanitizer is in charge of sanitizing the data blocks corresponding to the sensitive information (personal sensitive information and the organization's sensitive information) in the file, transforming these data blocks' signatures into valid ones for the sanitized file, and uploading the sanitized file and its corresponding signatures to the cloud.

(4) KGC: The KGC is trusted by other entities. It is responsible for generating system public parameters and the private key for the user according to his identity ID.

(5) Proxy: The Proxy is a public verifier. It is in charge of verifying the integrity of the data stored in the cloud on behalf of users.

(6) Cloud Server: The Cloud Server maintains and coordinate the Hacking Information .If any file gets Hacked it notifies the user stating that someone hacked your account and it also instantly recovers and stores the recovered file into the database 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 (EHRs) system, the cloud file strength contain 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.



(Fig. 1 System Architecture)

Design Goals

To efficiently support data sharing with sensitive information hiding in identity-based integrity auditing for secure cloud storage, our scheme is designed to achieve the following goals: 1) The correctness:

a) Private key correctness: to ensure that when the KGC sends a correct private key to the user, this private key can pass the verification of the user.

b) The correctness of the blinded file and its corresponding signatures: to guarantee that when the user sends a blinded file and its corresponding valid signatures to the sanitizer, the blinded file and its corresponding signatures he generates can pass the verification of the sanitizer.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

c) Auditing correctness: to ensure that when the cloud properly stores the user's sanitized data, the proof it generates can pass the verification of the Proxy.
2) Sensitive information hiding: to ensure that the personal sensitive information of the file is not exposed to the sanitizer, and all of the sensitive information of the file is not exposed to the cloud and the shared users.
3) Auditing soundness: to assure that if the cloud does not truly store user's intact sanitized data, it cannot pass the Proxy's verification.

Auditing System Architectures

To enable a continuous evidence extraction and transmission, a communication model is required. An auditor's system can be efficiently connected to auditees' systems, for example, by using the Simple Object Access Protocol to exchange messages, or by using the Common Object Request Broker Architecture as a middleware to gather information from heterogeneous auditees' applications . Auditrelevant data can be transferred at predetermined intervals and then stored in supplementary databases, for instance, in audit data marts . Audit data marts are small, mostly auditee-independent data repositories in which relevant data is automatically stored, enabling realtime data access and automated data analyses . Aside from individual mechanisms to gather audit evidence, researchers have developed several comprehensive CA system architectures. A monitoring and control layer can be implemented as an independent auditing system . This system forms an overlay on top of a set of existing systems and utilizes a middleware layer to provide integration between loosely coupled applications such as auditees' service applications and legacy systems . Data from integrated applications can be extracted and compared to a predefined auditing rule-set, and detected violations might automatically trigger an alert. This system is owned and operated by the auditor, thus data retrieved can be presumed to be tamper-proof . Applicability of monitoring and control layers in CC contexts might be limited due to distributed cloud infrastructures. Besides, agent-based CA architectures are common in literature and practice. Under this architecture, a digital agent is initiated to represent a certain audit procedure and dispatched to different auditees' systems . A flexible (e.g., platform independent) and adaptable (e.g., agent can be deployed as required) agent-based architecture facilitates gathering audit evidence in distributed and heterogeneous auditees' systems . Hierarchically structured teams of agents will perform planned audit operations, for example, interacting with an auditee's system and retrieving necessary audit evidence, testing effectiveness of business processes, or mining data to analyze and identify fraud behavior . In contrast to usage of monitoring and control layers in cloud contexts, agent-based CA architectures enable a flexible deployment and transmission of agents across different cloud infrastructures and locations. Furthermore, CA can be implemented as a set of web services that reside within an auditor's computing environment . Each auditing function is therefore represented as a web service which can be invoked to continuously audit an auditee's system . Usage of web services for auditing enables new business models for auditors, for example, cloud customers paying a service fee for invoking an auditor's web service to continuously retrieve assurance reports. In this regard, an incident detection web service was developed to enable customers to observe individual specified security and monitoring policies . When performing CA, a huge volume of data, exceptions and reports may be generated, thus threatening audit efficiency. To counteract this issue, it is recommended to implement decision support systems (DSS). Such systems might enhance CA by aggregating information from many different sources (e.g., agents or minded data), reacting on auditee reports, and by efficiently and automatically deciding to take actions or to alert the auditor. Consequently, DSS ultimately reduce workload of auditors. Future DSS may even evolve to intelligent and adaptive audit process systems, which automatically adjust audit tests based on gathered data and unexpected events. Interviews revealed that DSS are currently not used during CSC processes. Nonetheless, auditors endorse the concept of using these systems to support and to automate their auditing.

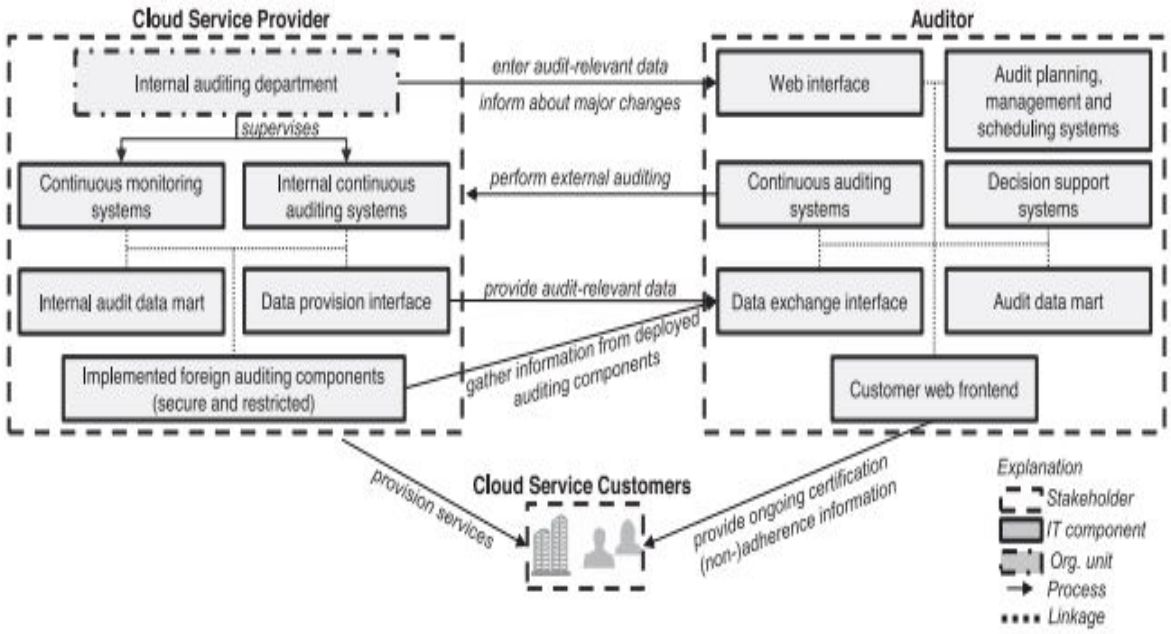
ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019



(Fig. 2 Auditing System Overflow)

MODULES

(A) File Uploading and Activation

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.

(B) Data Integrity and Auditing

Data integrity auditing scheme hat 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.

(C) Sensitive Information Sharing

Sensitive information hiding to ensure that the personal sensitive information of the file is not exposed to the hacker, and all of the sensitive information of the file is not exposed to the cloud and the shared users. This method not only realizes the remote data integrity auditing, but also supports the data sharing on the condition that sensitive information is protected in cloud storage.

(D) Generating Key Signature

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. However, it will make the whole shared file unable to be used by others.

(E) File Security and Recovery

If a file has been partially overwritten or otherwise compromised, the chances of any usable recovery are low, even with the best recovery software in the existing system. In our proposed work, we can easily recover the file while deleted files are inaccessible and are in danger of being overwritten, they can often be recovered**.**

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

III.PERFORMANCE EVALUATION

Performance of auditing.

With the different number of challenged data blocks, we respectively show the computation overhead of the Proxy and that of the cloud in integrity auditing phase . In our experiment, the number of challenged data blocks varies from 0 to 1,000.,AS shown , we see the that the computation overheads of challenge generation and proof verification on the Proxy side linearly increase with the number of challenged data blocks. The computation overhead of proof verification varies from 0.317s to 11.505s. Compared with the time of proof verification, the time of challenge generation increases slowly, just varying from 0.013s to 0461s. From Fig. we have the observation that the computation overhead of proof generation on the cloud side varies from 0.021s to 3.981s. So we can conclude that, with the more challenged data blocks, both the TPA and the cloud will spend the more computation overheads.

IV. CHALLENGES

Risk of Audit-Data Manipulation

Provision of audit-relevant data by a provider herself has one challenging drawback: the risk of data manipulation. Providers might modify provided data to assure ongoing certification adherence. Preventing cloud service providers to manipulate or euphemize audit-relevant data is an important prerequisite to ensure that CA is trustworthy and reliable. Consequently, providers have to establish secure logging mechanisms which achieve a high degree of log integrity and confidentiality. In order to achieve this, we can build on findings from research area of cloud forensics. Cloud forensics is defined as the application of scientific principles, technological practices to reconstruct past cloud computing events through identification, collection, preservation, examination, interpretation, and reporting of digital evidence. Researchers have proposed various procedures to deal with challenges of cloud forensics (i.e., malicious cloud service providers manipulating log files), ultimately enabling third party investigators to collect and analyze relevant data . Cloud service provider can implement appropriate log adapters to extract and transfer log entries from different logging sources (e.g., hypervisor) to a central logging component . This central logging component transforms log entries into a secure, encrypted and uniform log type. To prevent internal log manipulation, a trusted third party module (e.g., hardware or virtual module) can be implemented that provides secure log encryption functions. Similar, various schemes are proposed (i.e., homomorphic encryption) and evaluated using open-source cloud computing platforms to ensure privacy and confidentiality of log data.

Further on, one way of revealing data manipulation is to establish a chain of custody for digital evidence , which represents a roadmap that shows how data was collected, analyzed, and preserved in order to be presented as evidence in court. Moreover, several procedures are recommended to gather trusted audit-relevant data, including remote data acquisition over trusted and secure channels, usage of management planes, preforming live forensics on systems in running state, as well as snapshotting a clone of a virtual image among others (cf., for a detailed comparison). Nonetheless, cloud forensics procedures will vary according to service and deployment model of cloud computing. For example, Software- and Platform-as-a-Service models inherit very limited control over process or network monitoring, whereas in Infrastructure-as-a-Service settings some forensic friendly logging mechanism might be deployed. Future research should evaluate how existing procedures from cloud forensics research can be applied to enable CA.

Availability Issues

Ensuring availability refers to ensuring timely and reliable access to and use of information . In the context of CA, availability of cloud systems and provided interfaces has to be ensured. First, performing continuous monitoring and auditing process (e.g., ongoing data gathering, analysis and aggregation operations) might have a substantial performance impact on cloud services. Likewise, failures in these operations might lead to disturbance of cloud service operation. Hence, CA might threaten cloud service availability. Second, when audit-relevant data is provided via defined interfaces, providers have to assure availability of them. Attackers might target interfaces, for example, by performing distributed denial of service attacks to disturb the process of CA. In worst cases, this might lead to non-adherence of CSC criteria, since auditors are lacking corresponding audit information. Finally, providers have to assure that provided user interfaces for customers are available.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

V. RESULT AND ANALYSIS

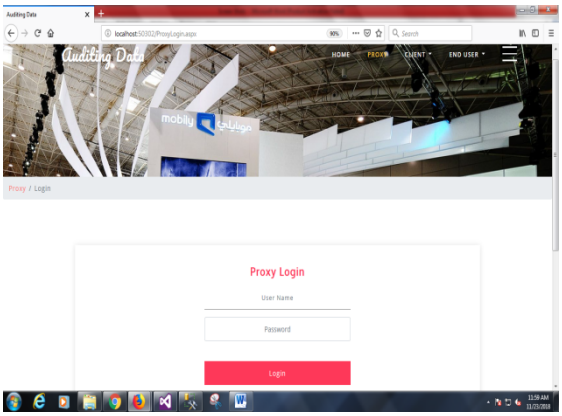
Login Page

The Following figure shows the overall Web page of the proposed system. It consists of proxy cline and end user credentials.

(Fig 3 : Login Page)

Proxy Login

The fig. 4 consists of login page of proxy. It consists of proxy credentials and by logging into proxy it maintains the user file activation process.



(Fig 4: Proxy Login)

Client Login

Fig.5 displays the client login page. Here client can enter their credentials and can upload their file by activating the file and can also check the data integrity of the file which has been uploaded.

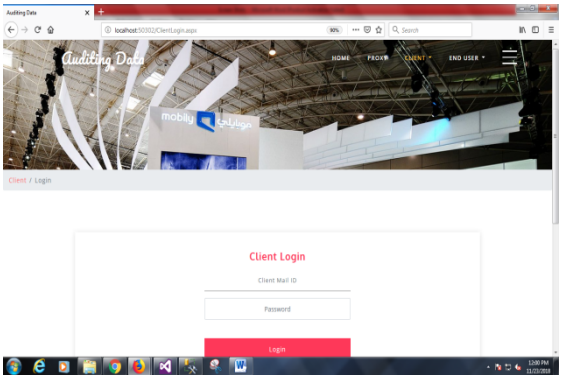
ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

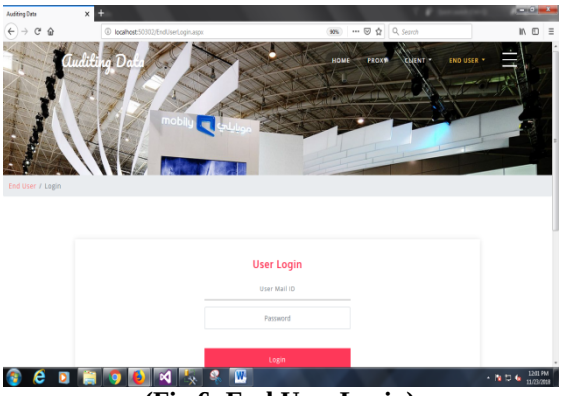
Vol. 7, Issue 2, February 2019



(Fig 5: Client Login)

End User Login

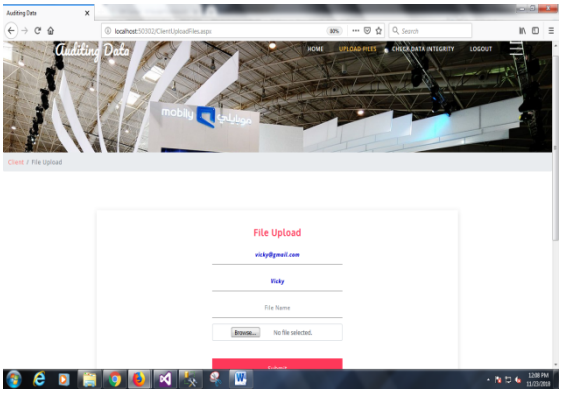
Fig. 6 describes about the end user login where the end user can enter their credentials and either view or download the data file from the page by getting the secret key for the file from the KGC.



(Fig 6: End User Login)

File Upload

Fid. 7 shows that, user can upload their file into the cloud database into the encrypted format. Already Existing File name can't be uploaded into the database.



(Fig 7: File Upload)

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

VI. FUTURE RESEARCH

In this paper, the data owner independently upload the data to the Cloud and data will be monitored by an third party auditor(TPA). However data privacy may be leaked to the TPA during the checking process, which may cause financial loss for the users who have stored confidential or sensitive data on cloud servers, which is an disadvantage and an protective method should be considered as the future work to overcome this drawback.

VII. CONCLUSION

This Paper proposed 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.

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.