|| Volume 6 || Issue 7 || July 2021 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

IDENTITY-BASED PROXY-ORIENTED DATA UPLOADING AND EDGE DATA INTEGRITY CHECKING IN EDGE CLOUD

Manchala Naveen Kumar[1] and K.Ramesh[2]

Research Scholar, Dept. of Computer Science Engineering, Chintalapudi Engineering College, Chintalapudi[1]

Associate Professor, Dept. of Computer Science Engineering, Chintalapudi Engineering College, Chintalapudi[2]

Abstract: - Great demand over remote data accessibilities with more flexible and efficient manner people tend to use cloud computing architecture more and more these days and became a trending technical platform. Especially at the computing services in handling distributed information systems demands more reliable client data processing more securely. Today's modern strategies need to adopt lightweight remote data access support system that processes data more effectively and efficiently. So by adopting edge computing we could be in a situation to contribute IT services over distributed platforms and makes us provide vendor services in a wider range in fulfilling service level agreements for cloud users with more and more effective strategies. So we recommend this Data integrity over edge computing platform that strives to achieve vendor side inspection and avoid malicious attacks to achieve service vendor satisfaction in a better way. So primary emphasis in handling data integrity evaluation policies efficient way to solve security issues that are over platforms. Thus policies should be framed in such a way computationally strict standards have to be adopted in the process of evaluation of client's authorization and client service transactional interactions towards secure availability of Data services over clouds.

Keywords:- *Edge data integrity, edge computing, service vendor, privacy protection.*

I INTRODUCTION

Huge data that has to serve remote data access needs to be organized computationally to effectively provide accessibility along with that we may need to focus on security parameters so that this remote access of data by remote users needs to get evaluated and with the proper identity-based digestion so that the data confidentiality can be maintained more effectively. To handle the above-said problem we may need to focus on security standards that is when cloud client attempts to access the data needs to get verified over their integrity and confidentiality order to provide the Data Services more efficiently. In another way, this leads to limited capacity and uses when we attempt to increase the data integrity policy strategies with more and more high levels of standards. So it is a crucial factor that we may need to care about the effective implementation of integrity evaluation along with efficient access of cloud data that is under service. To adopt new policy strategies that help us to establish a good system effectively and efficiently handle remote data access call that comes from both authorized and malicious users so that malicious data uses attack should be blocked which improves the security standards.

Motivation:

In edge computing public infrastructure, the client access the remote data needs to pass through data integrity strategies which of course intern increases the reliability of data contributed by data owners. The legalistic approach of scrutinizing data access of remote users should be driven with a key agreement policy so that motives there should be mapped with their proper identity key which will be verified and evaluated access remote data. So this key agreement strategy is been organized by the cloud computing administrative system very effectively by incorporating the auditor's role. As well

system should also get incorporated with a proxy module to authorize respective remote uses so that data services can be contributed more efficiently. So the system should be in a situation to handle data privacy leakages like remote data access by malicious users over a huge volume of data. Show within this cloud infrastructure should incorporate public protocol to perform certificate management effectively so that remote data access is delegated to the authorized remote data using an extreme certificate evaluation policy. So our cloud system infrastructure should maintain secure mechanisms like generating certificates, delegating tokens, certificate revocation, certificate renewals so that remote and uses will be permitted with less computational capacities and key cryptosystem enables typical certificate management system in data uploading of remote data integrity access can be driven more effectively and efficiently.

II LITERATURE SURVEY

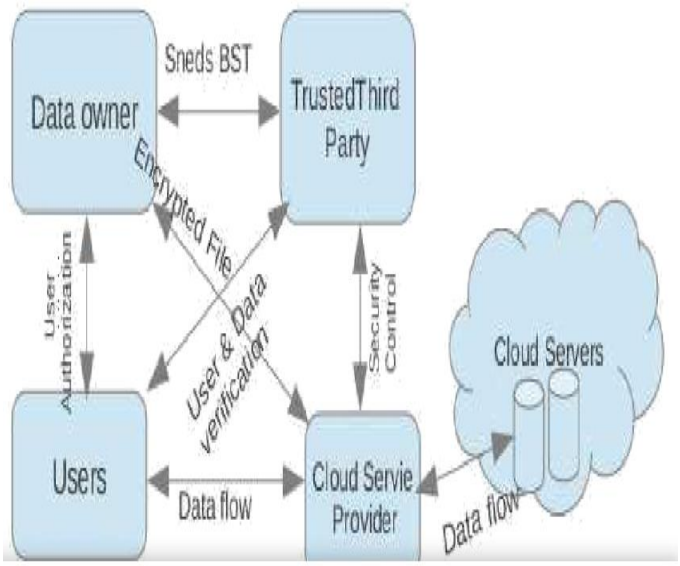
"Security Challenges for the Public Cloud, IEEE":

Focusing on the upcoming enhancements administrating services over Cloud Computing domain computational operational it is are been entertained in such that area of software as a service is been empowered with the new attribute of security requirements. Based on the operational nature of cloud computing that is a request that could range from a user on towards the cloud server computational resources are being effectively administered with the wide scope in drastic resource deployment and came to an effective utilization policy. The fundamental operational activities shouldn't get disturbed when we attempt to enhance the computational services that got delivered or outsourced both to an independent body d or a corporate division committed to specific commercial and managerial terms effectively. These logical computational strategies need to get administered by cloud service providers as it involves commercial and managerial statistics of the system as well as needs to randomly adopt resource deployment in rapid timelines. So this recommended Cloud Service Provider infrastructural and managerial capability with sophisticated computational methodologies should play an effective part towards security both within and outside the system limits and should also handle privacy attacks from and malicious users which may reduce the reliability and trustability over the system

"Enabling Identity-Based Integrity Auditing and Data Sharing With Sensitive Information Hiding for Secure Cloud Storage"

Maintaining sensitive and private information is of crucial importance in facilitating patient control towards access privileges of their health records without compromising on security e factors makes is to move to adopt a typical encryption process model before it is been outsourced to the Cloud Service. Handling electronic health records has great demand when we accommodate them in a cloud computing environment which could be driven with the patient-centric model of medical data exchange is kept available for outsourcing to a third-party service provider authorized parties. We may need to emphasize several security risks over the private information of the data owner provided content needs to get empowered with privacy, scalability, index key management, trustable data access is been contributed effectively. In this research, we also focus on many data owner count situations and bifurcate the users into a variety of domain-based security models which in turn minimizes the complexity in maintaining key Management processes.

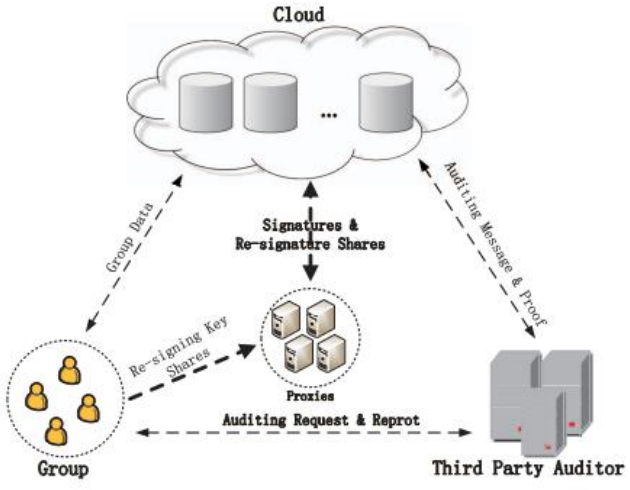
"A Design for Scalable and Secure Key-Value Stores"



In a cloud computing environment, cloud-based data utility applications need to maintain reliable and scalable data storage accumulation main to emphasize much on the cryptographic conversion of the plaintext forms into ciphertext forms. To enhance the security standards we may need to emphasize encryption-based mechanisms and also providing flexible data utilization schemes data users may rely on third-party vendor personalities for the data stored by the data contributor. Data contributor data needs to get encrypted and kept ready for service for data consumers wherein the data can be restored into the compatible forms by using a relevant decryption mechanism. This third-party vendor key management facilitates flexible and secure data integrity approaches to power the cloud data stored in encrypted systems.

"Efficient integrity auditing for shared data in the cloud with secure user revocation"

Especially when we focus on the security measures that have to be taken over at the cloud server we may need to primarily focus on three crucial approaches of intimidation to enhance the integrity of the cloud data sharing process.



Firstly in the environment of the cloud server, private sensitive shared data may be spoiled due to manual errors or physical system issues or software handling mechanisms needs to safeguard the data from malicious users to increase trustability. In such a scenario reassignment of signatures to the corresponding segmented blocks will be carried to handle privacy needs. In this process, the cloud server administrator may need to identify an intruder and revoke it from the service access mechanisms.

III SYSTEM ANALYSIS

Existing System:

Public cloud systems data owner attempts to upload data into the cloud storage so that it will be kept for service to manage remote data users. So all the remote data users need to get managed properly all data access transactions should be done securely. To achieve we need to map transactions with an appropriate user identity so that the remote data should be properly authorized. In certain circumstances, we may need to facilitate proxy to access data and even this delegation needs to properly.

Disadvantages of the existing system:

- No proper dynamic key agreement strategies were adopted.
- Lack of Reliability over data owners stored data.
- Lack of efficiency over a key generation.

Proposed System:

We proposed a new system that adopts a lightweight remote data access support system that processes data more effectively and efficiently. So by adopting edge computing we could be in a situation to contribute IT services over distributed platforms and makes us provide vendor services in a wider range in fulfilling service level agreements for cloud users with more and more effective strategies. So primary emphasis in handling data integrity evaluation policies efficient way to solve security issues those are over platforms. So we recommend this Data integrity over edge computing platform that strives to achieve vendor side inspection and avoid malicious attacks to achieve service vendor satisfaction in a better way. Thus policies are framed in such a way computationally strict standards have to be adopted in the

process of evaluation of client's authorization and client service transactional interactions towards secure availability of data services over clouds.

Advantages of the proposed system:

- This dynamic key agreement system is more efficient and effective.
- Data owner's data that got stored in the cloud server is under secure remote access transactions.
- The proposed protocol generates a dynamic eliminates malicious user attack over proprietary data of data owner.

IV IMPLEMENTATION

There are four modules in this project. They are:

- Data Owner
- Key Generation Center
- Trust Party Authority
- Cloud Server

Data Owner:

The primary objective of this Data Owner module is to push proprietary data into the cloud Store and readily kept under remote data access service. The data owner needs to get projected and organized by using a private key generated by the key generation center. Using this DO can log into his account and upload desired files into the cloud data server. All the audit requests that came for data of data owners towards TPA will get reported at the data owner's end then file access will be granted.

Key Generation Center

The primary objective of Designing a key generation Center is to generate the dynamic key to facilitate an identity-based secure system through which all other relations will be evaluated with the private key generated by KGC towards data owners and users.

Trust Party Authority

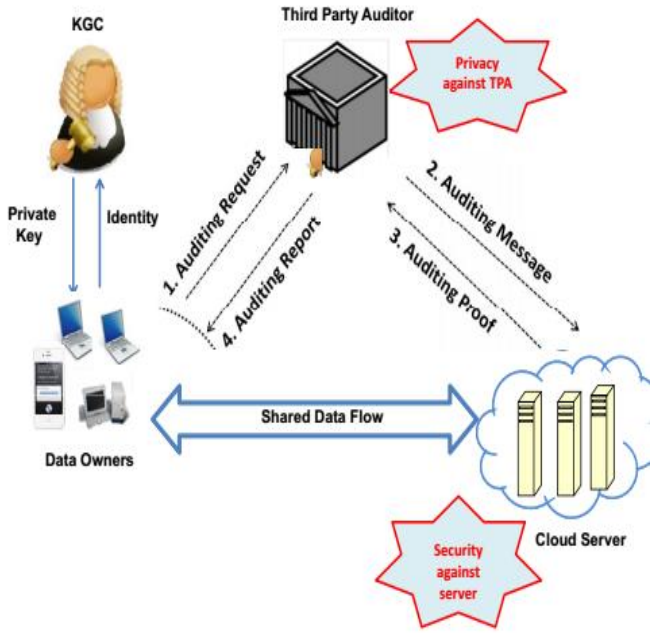
We may need to aim for a proxy authority that made us create a trust authority module in the proposed system So that this module will register requests to cloud server towards identity proof for the entire data user requests. After identity proof evaluation, the TPA module well grants data access upon data owner acceptances for all the requests.

Cloud Server

In this module, the cloud will authorize both the owner and the user. Views all the requests from the users and provides keyword search control. This module can view all the uploaded files and the details and also finds who try to attack the files maliciously using a key evaluation protocol ., sending proof to TPA.

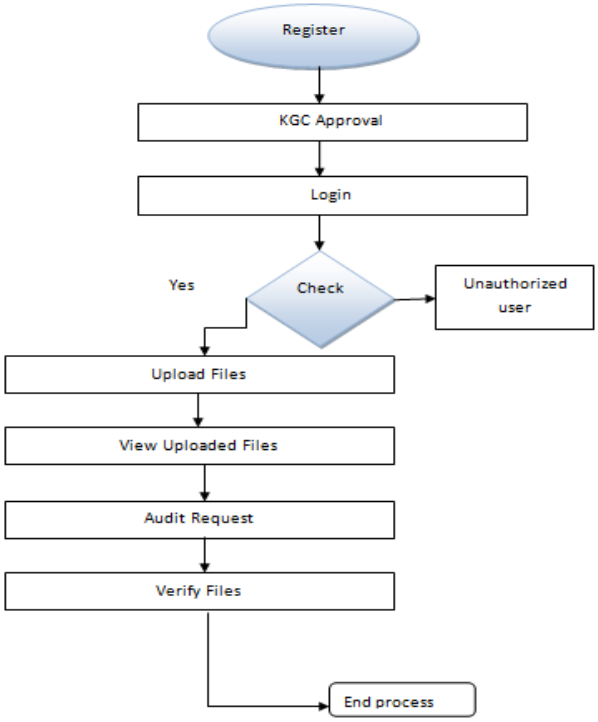
V SYSTEM DESIGN

Architecture diagram:

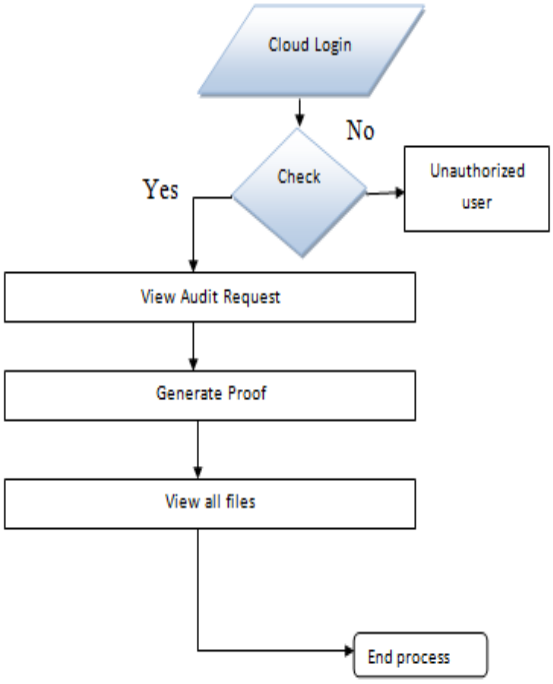


Data flow diagram:

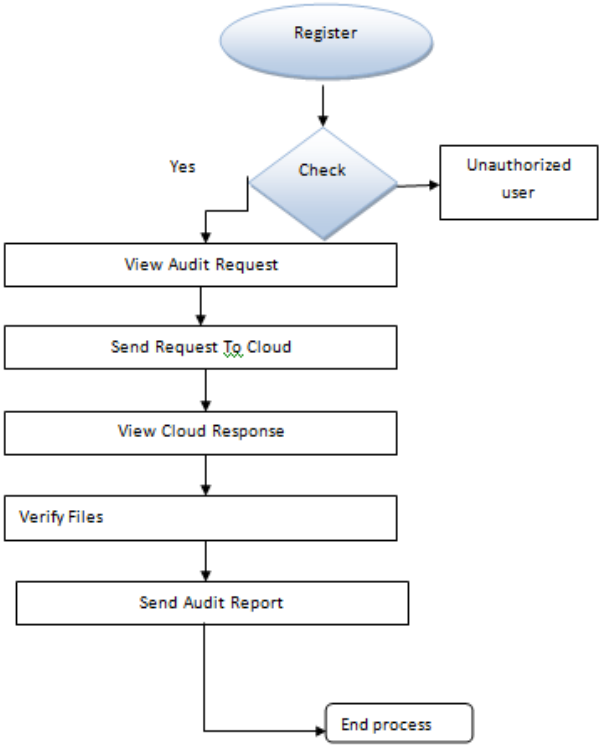
Data Owner:



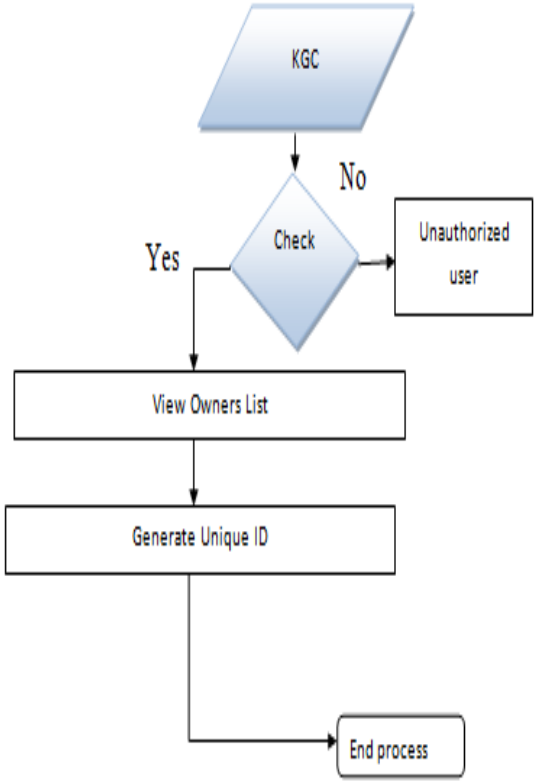
CLOUD:



TPA:

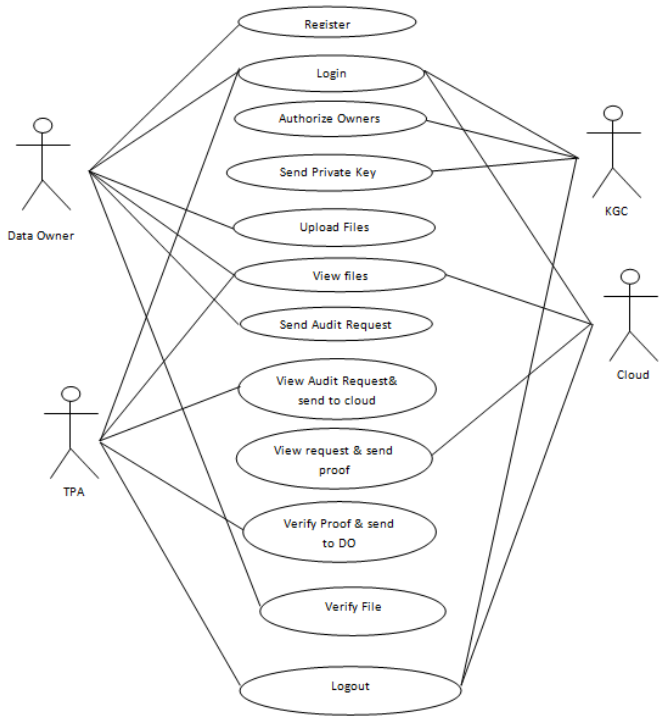


KGC:



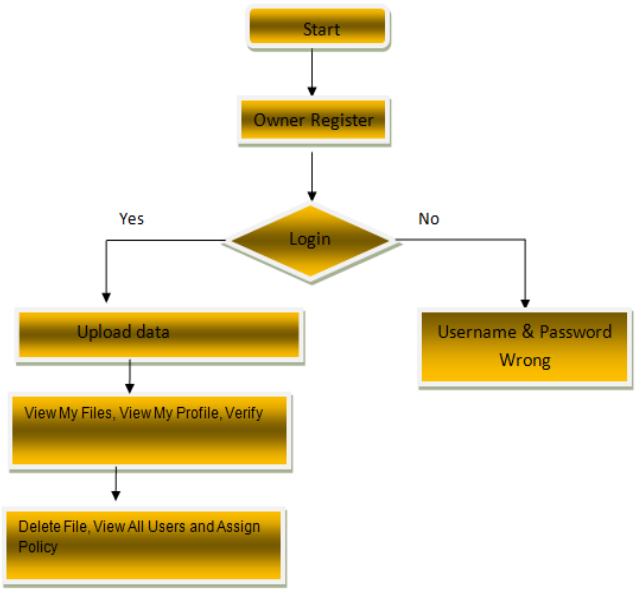
UML Diagram

Use case diagram:

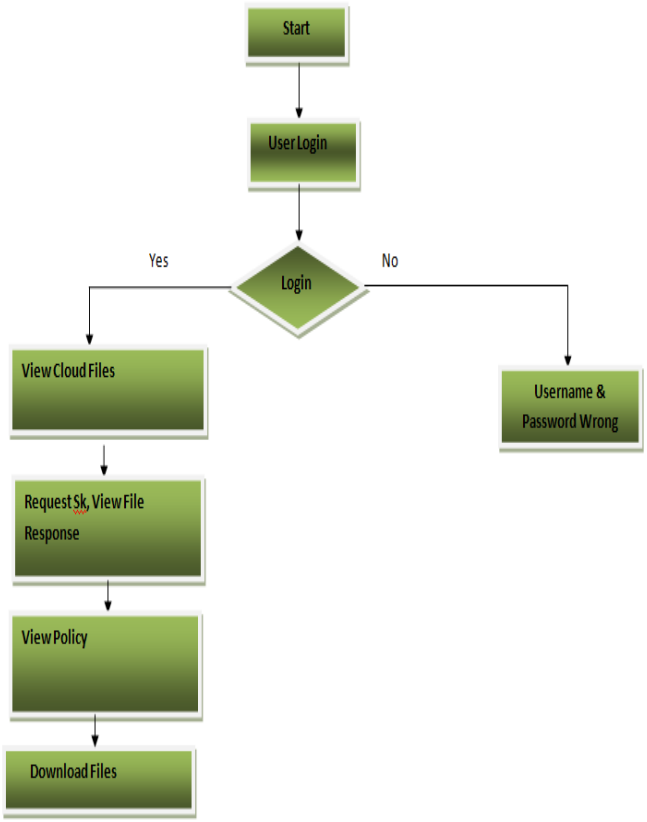


Flow Chart:

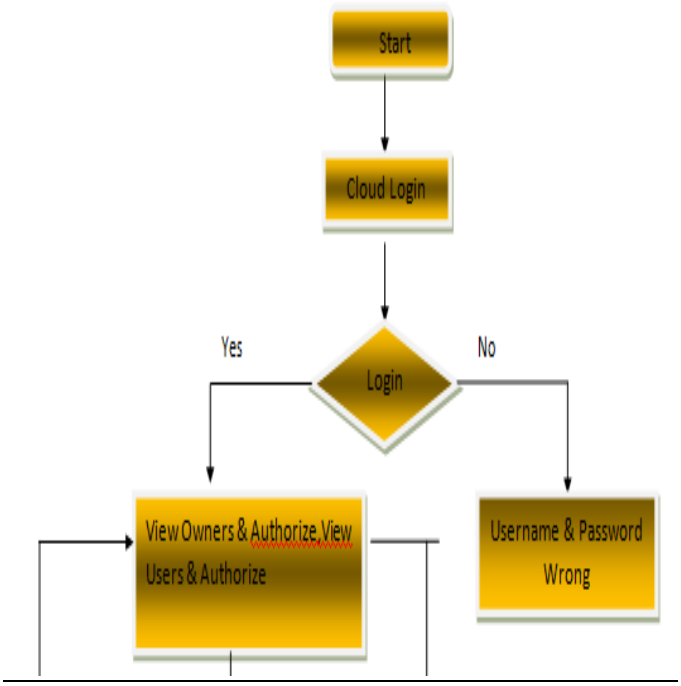
- **Flow Chart: Data Owner**



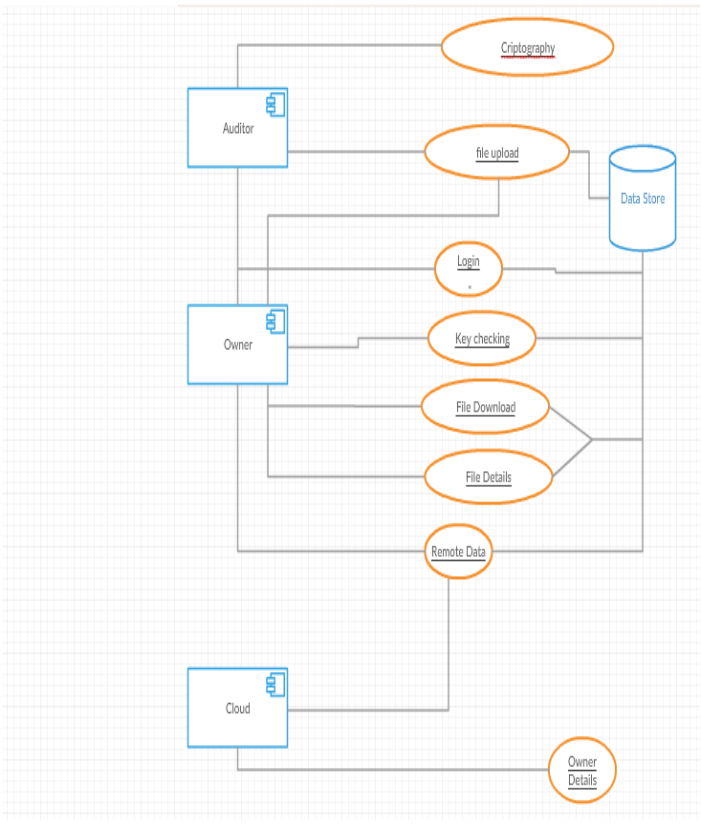
- **Flow Chart: User**

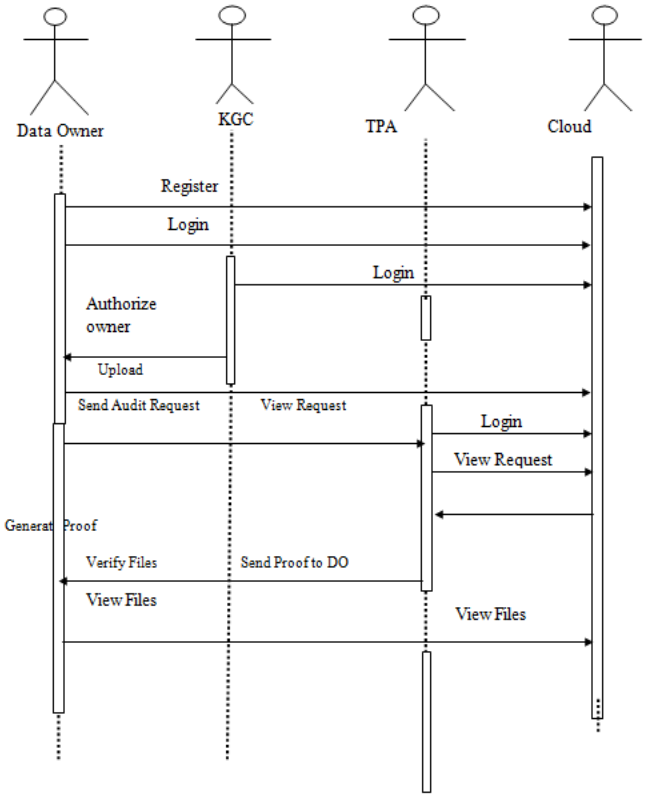


- **Flow Chart: Cloud Server**



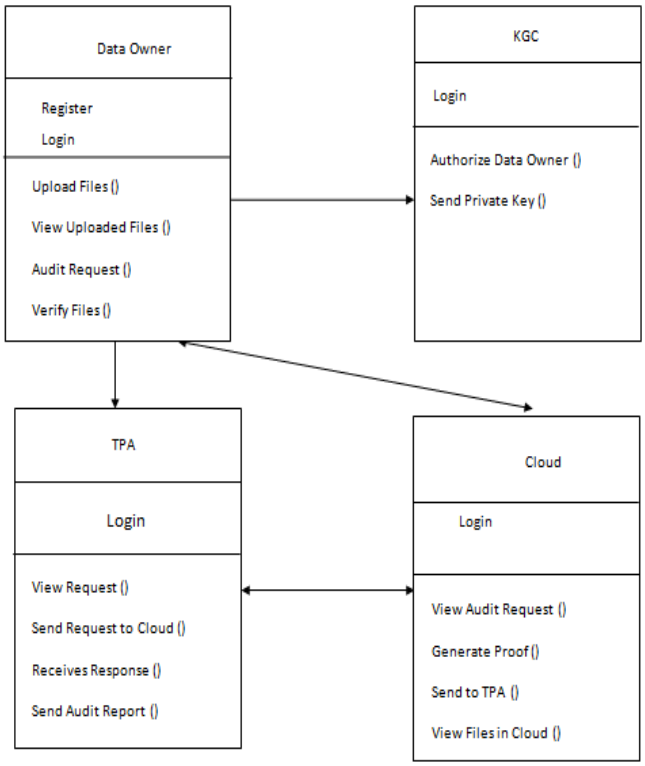
Module Diagram :-

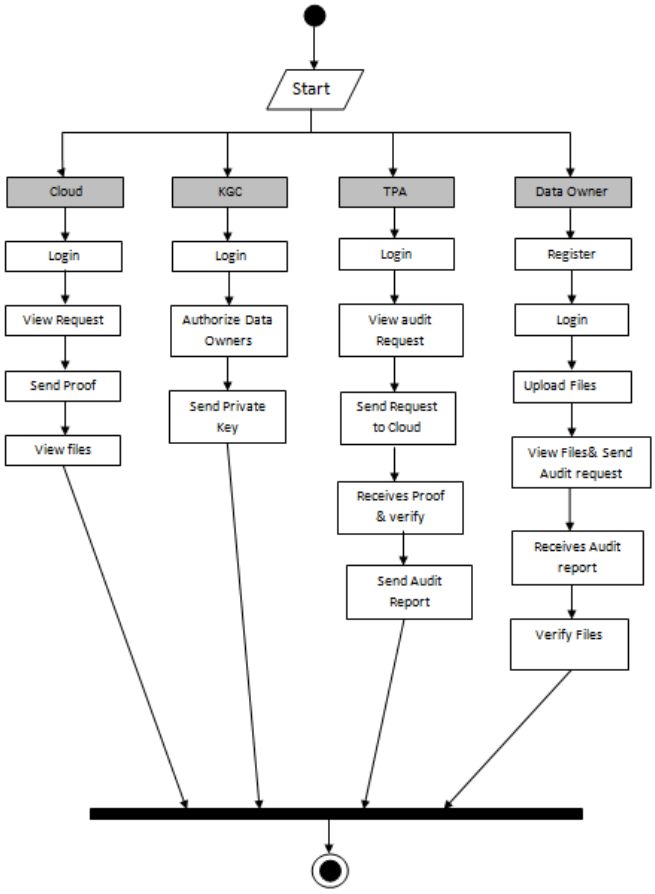




Activity diagram:

Class diagram:

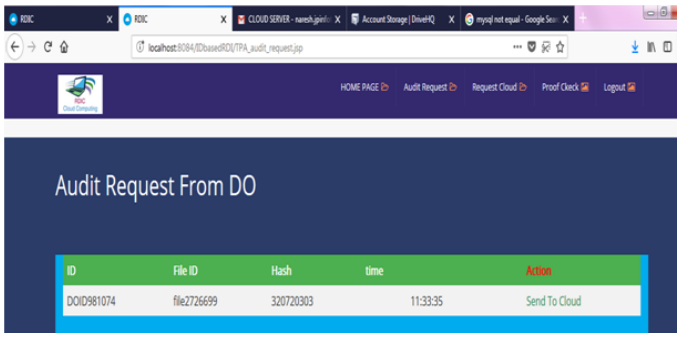


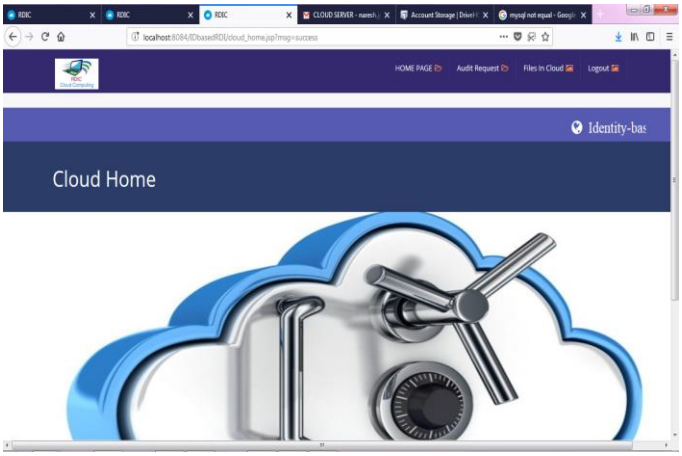


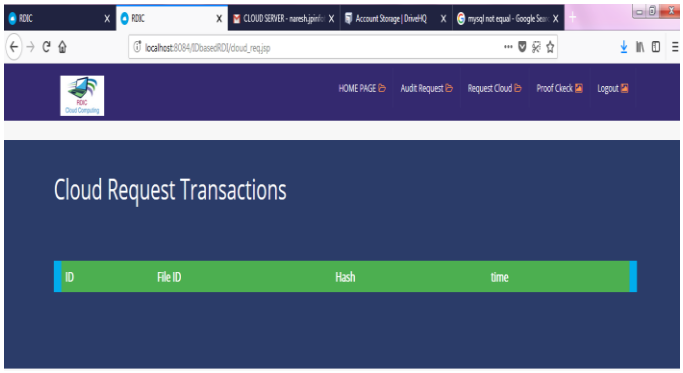
Sequence diagram:

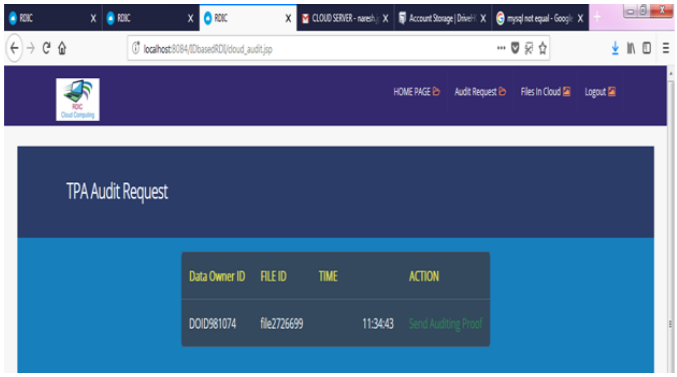
|| Volume 6 || Issue 7 || July 2021 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH AND ENGINEERING TRENDS

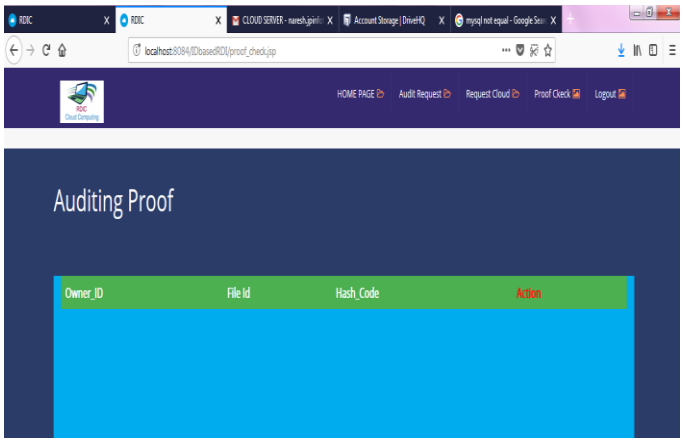
VI PROJECT EXECUTION PROCESS

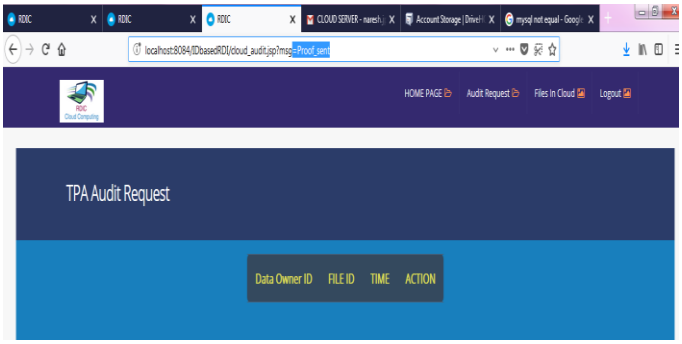


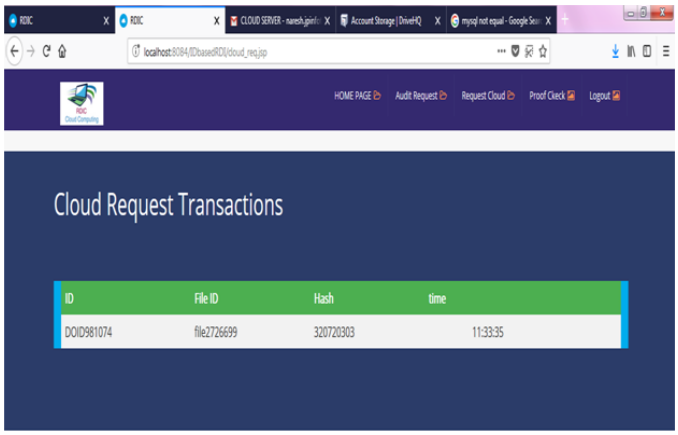


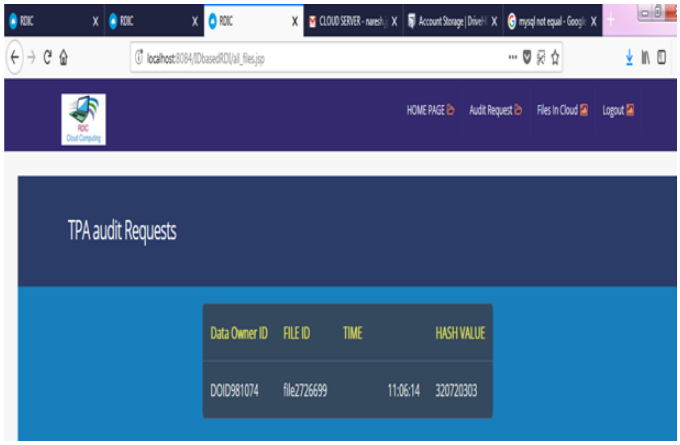


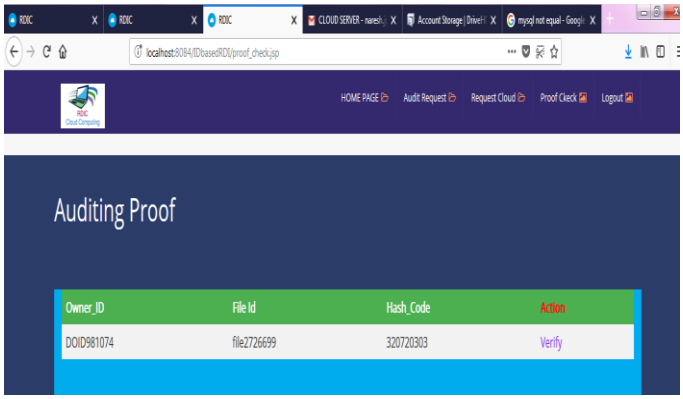


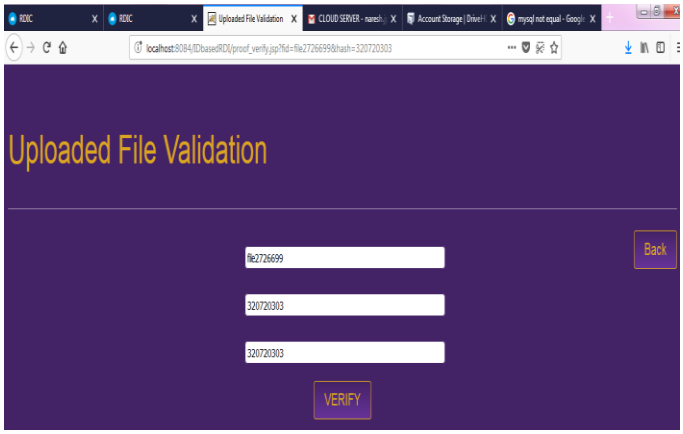


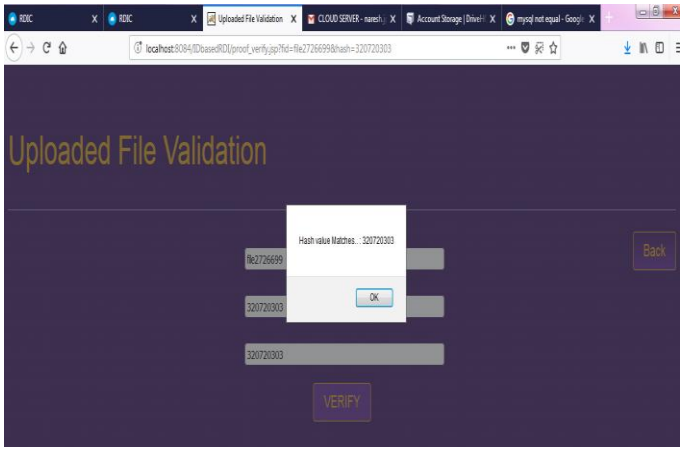


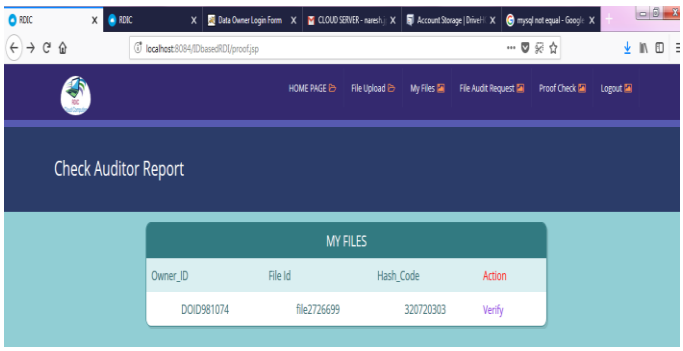












VII CONCLUSION

In this project we successfully introduced a novel security mechanism so that remote users could able to avail themselves of Data Services more securely and effectively, Data owner's data is facilitated with confidentiality maintained in a much better way. By using this novel high secure system model we tried to bring up key agreement policy effectively identity could be maintained dynamically in a most effective way. This key agreement management helps us to authorize remote clients with the highest security standards. By using this novel approach we attempt for high data privacy standards, data reliability, and confidentiality over preparatory data could be maintained under service with high security, as well as remote users get benefited inefficient manner.

Future Enhancement:

Additionally, we could attempt to deal abnormal situation handling process like glass breaking mechanism over high secure cloud system so that we could handle the miscellaneous loss of keys at data proprietors end. This glass-breaking mechanism greatly helps in serving the remote users most effectively without any service breakage even though there is a mistake happened at the data owner's end due to their proprietary data-associated aggregated key loss.

REFERENCES

[1] Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, "Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing," IEICE Trans. Commun., vol. E98-B, no. 1, pp. 190–200, 2015.

[2] Y. Ren, J. Shen, J. Wang, J. Han, and S. Lee, "Mutual verifiable provable data auditing in public cloud storage," J. Internet Technol., vol. 16, no. 2, pp. 317–323, 2015.

[3] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures for delegating signing operation," in Proc. CCS, 1996, pp. 48–57.

[4] E.-J. Yoon, Y. Choi, and C. Kim, "New ID-based proxy signature scheme with message recovery," in Grid and Pervasive Computing (Lecture Notes in Computer Science),

vol. 7861. Berlin, Germany: SpringerVerlag, 2013, pp. 945–951.

[5] B.-C. Chen and H.-T. Yeh, "Secure proxy signature schemes from the weil pairing," J. Supercomput., vol. 65, no. 2, pp. 496–506, 2013.

[6] A.Juels, and B. S. K. Jr. Pors, proofs of retrievability for large files.Proc. of CCS 2007, 584-597, 2007.

[7] H. Shacham, and B. Waters, Compact proofs of retrievability. Proc. of Cryptology-ASIACRYPT 2008, LNCS 5350, pp. 90-107, 2008.

[8] G. Ateniese, S. Kamara, J. Katz, Proofs of storage from homomorphic identification protocols. Proc. of ASIACRYPT 2009, 319-333, 2009.

[9] A. F. Barsoum, M. A. Hasan, Provable multicopy dynamic data possession in cloud computing systems, IEEE Trans. on Information Forensics and Security, 10(3): 485–497, 2015.

[10] S. Ohata, Y. Kawai, T. Matsuda, G. Hanaoka, and K. Matsuura, "Re-encryption verifiability: How to detect malicious activities of a proxy in proxy re-encryption," in Proc. CT-RSA Conf., vol. 9048. 2015, pp. 410–428.