International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 11 | Nov 2022 www.irjet.net p-ISSN: 2395-0072

SECURE FILE STORAGE IN THE CLOUD WITH HYBRID ENCRYPTION

Dr. Mohammed Bakhar[1], Arshiya Umara Hussain[2]

[1] *Professor, Dept. of Electronics and Communication Engineering, Guru Nanak Dev Engineering College, Karnataka, India*
[2]*Student, Dept. of Electronics and Communication Engineering, Guru Nanak Dev Engineering College, Karnataka, India*

Abstract - *An increasingly common use of cloud computing is cloud storage, which allows businesses and individuals to outsource their data whenever they need it. However, users may not have full confidence in cloud service providers (CSPs). This is because it is difficult to determine whether regulatory beliefs for data safety are being met. Consequently, it is important to progress effective authentication procedures that increase statistics holders' trust in cloud storage. This white paper introduces a new public audit program for secure cloud storage based on Dynamic Hash Tables (DHT). A new two-dimensional data structure called DHT stores data quality information in the Third Parity Auditor (TPA). Dynamic log analysis, the proposed technique moves legitimate information from his CSP to the TPA, significantly reducing computational cost and communication overhead, in contrast to previous work. On the other hand, our approach can also achieve higher renewal efficiency than prior art schemes by exploiting the structural advantages of DHT. We extend the scheme to support data protection by combining a public-key-based homomorphic authenticator with a TPA-generated random mask and using the BLS sum-signing technique for batch verification. We formally state the security of the proposed system.*

Key Words: Cloud Storage, Data Security, Hybrid Cryptography, Encryption, Decryption, etc

1. INTRODUCTION

An essential component of cloud computing, Cloud Garage aims to use highly virtualized infrastructure to provide consumers with potent, on-demand, fact-based goods. More and more businesses and people are outsourcing their statistical garages to expert cloud service providers due to the low cost and great performance of cloud garages, which reflect the recent rapid growth of cloud garages and their connected technologies (CSPs) tend to Cloud storage. However brand-new and cutting-edge, still has a lot of security issues to solve. How to verify whether cloud garage devices and their issuers match the statistical security requirements of thieves is one of the major worries.

2. OBJECTIVE

The suggested paper complies with the cloud server's data center's implementation requirements for security. In order to fulfill the notion of data security, the concepts of splitting and merging are included. When a hybrid method is used in a cloud server, the distant server becomes more secure, assisting cloud providers in carrying out their duties more securely. The basic difficulty of separating sensitive data and access control is met for data security and privacy protection issues. Original data is transformed into ciphertext using the cryptography process. Symmetric-key and public-key cryptography are the two types of this encryption method. Consequently, only someone with permission may access the cloud server's data. Data in ciphertext is available to everyone. However, to do so once more, the decryption method must be applied to convert it to the original text.

3. SYSTEM ANALYSIS

EXISTING SYSTEM

It is known to introduce authenticated fact forms to collect dynamic audits. Common proxies are skiplist-based PDPs and MHT-based public audit systems. However, at some point in the update and validation process, high TPA computational costs and significant overhead can occur. Therefore, Zhu et al. provided a simple fact form called the Index Hash Desk (IHT) to report the alignment of blocks of information and help generate a hash fee for each block in the verification process. The structure of the IHT is a kind of one-dimensional array containing the index set, block type, model set, and random price.

A predominantly IHT-based structure can likewise condense storage reduces transmission and computation costs a house of record for auditing IHT usage within the TPA rather than the CSP. Unfortunately, due to the IHT's serial format, update operations (especially inserts and deletes) on the IHT are inefficient. This is because if N is the full multiplicity of all blocks, there will be an average N/2 element adjustment. Furthermore, during the course of an insertion or removal approach, the block number (Bi) of some blocks may inevitably change, thus regenerating the corresponding block tag. This is clearly

inefficient, computationally expensive for the user, and can result in pointless communication.

PROPOSED SYSTEM

There is a growing interest in auditing cloud storage. One of his earliest relevant papers is his Proof of Retrievability (PoR) by Juels et al. In 2007, we were able to checked the accuracy of the statistics deposited in CSP and use error correction code to reliably retrieve statistics. However, PoR is a typical private audit response and does not conduct an audit until after the third birthday celebration.

In the same year, Ateniese et al. First, Provable Information, a bona fide public testing scheme that uses RSA-based homomorphic tags and can remotely test the integrity of paginated statistics by randomly selecting some blocks from a file. Provided Ownership (PDP). As mentioned above, general audits can provide a more reliable audit suite compared to individual audits, and his independent TPA implementation can significantly reduce the client's pointless overhead. As a result, it is seen as more realistic and promising. Apart from that, besides data protection, batch verification and dynamic verification, cloud storage auditing has some major issues. The proposed system won't be that much economically costly as this application does not require any hardware part and interfacing with only one web server you need which you will get very easily and economically.

4. SYSTEM DESIGN

Mechanical design is the next level of improvement that establishes the general structure of the preferred system. Devices are made up of numerous interconnected subsystems. The analyst deals with these issues even when building a system as a collection of interconnected subsystems. New system requirements of the end consumer as well as the specifications involved in the system analysis.

Since the basic idea of object-oriented techniques for machine evaluation is to see devices as hard, fast-interacting objects, a larger machine can likewise be seen as a set of smaller interrelating subsystems. increase. object. When designing systems, the focus is on the elements that make up the device, and no longer on the tactics performed by the device, as in the outdated waterfall model, where lugs form an important part of the machine.

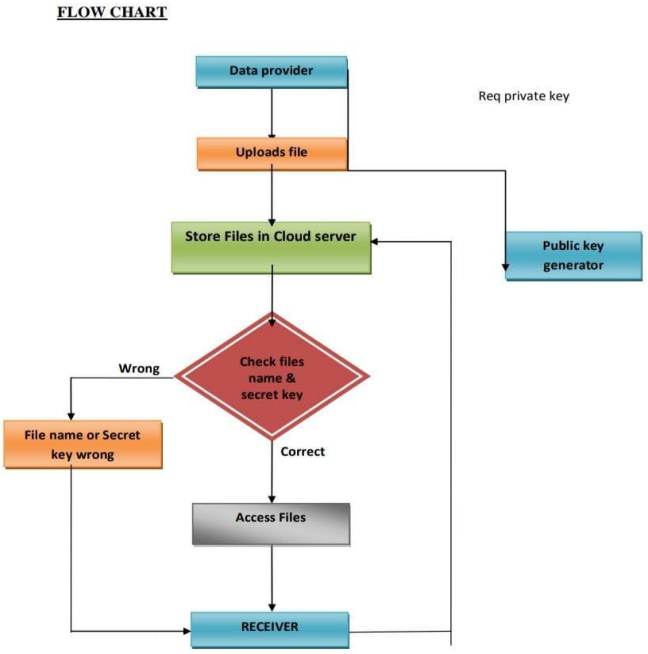


Fig 4.1 Flow Chart

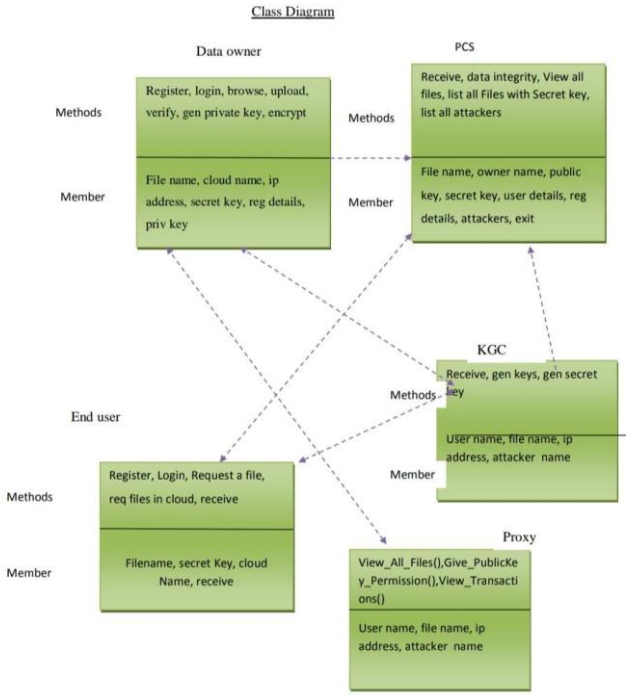


Fig 4.2 Class Diagram

Sequence Diagram:

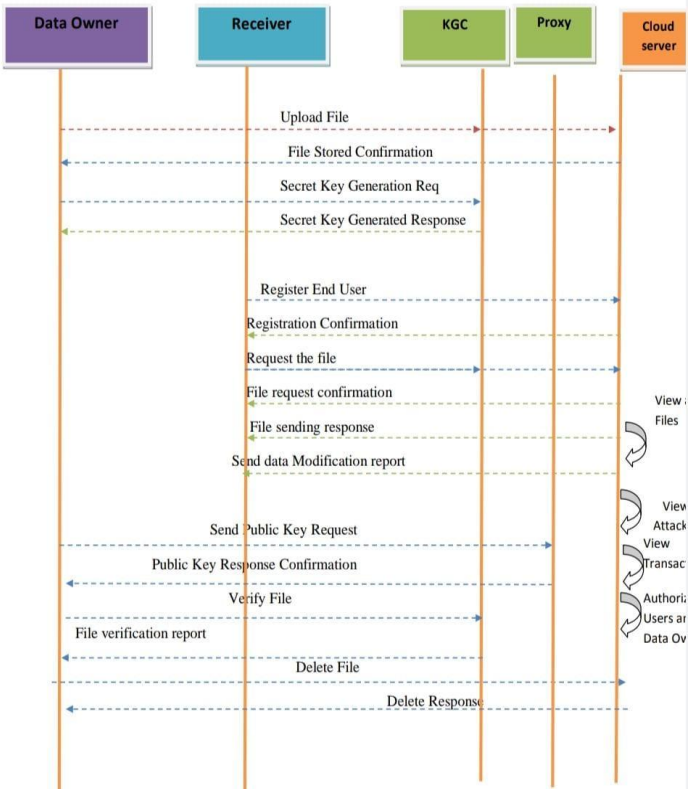
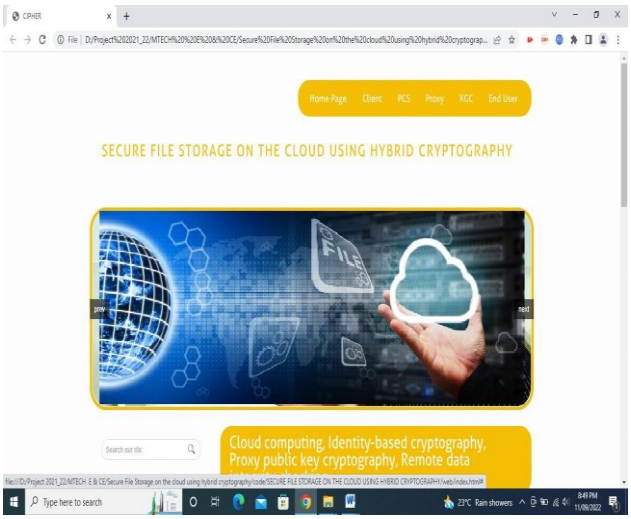
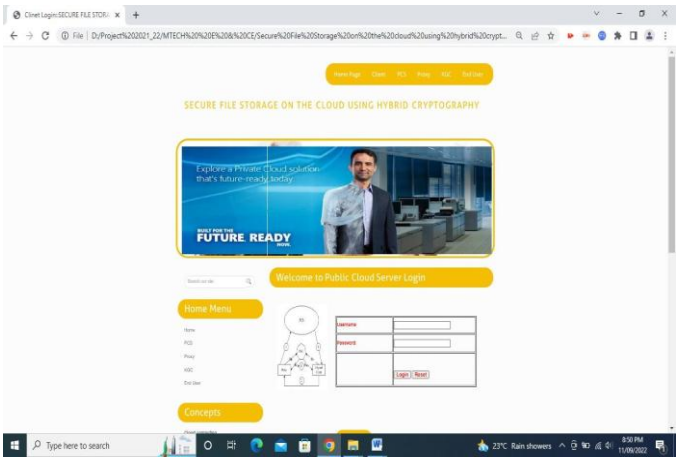


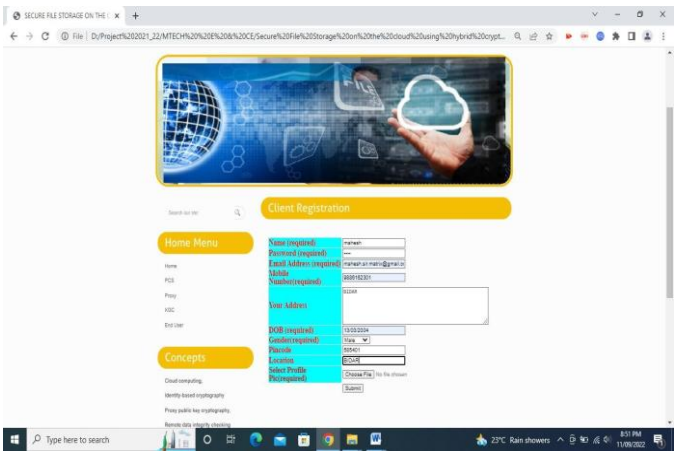
Fig 4.3 Sequence Diagram

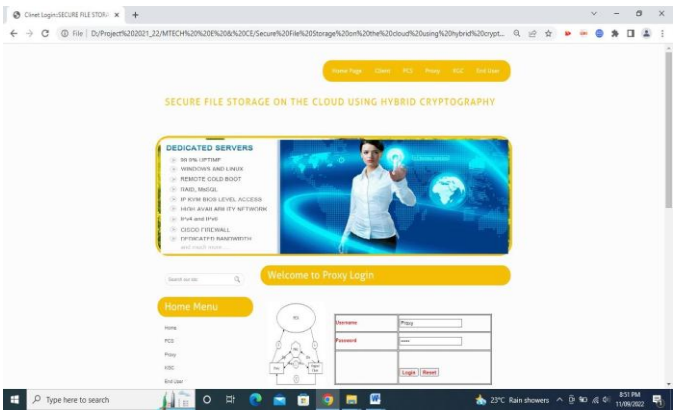
A random woodland has nearly the same hyper-parameters as a selection tree or a bagging classifier. Luckily, there is no need to combine a choice tree with a bagging classifier, as you could without difficulty use the Random woodland classifier. With a random woodland shape, you may additionally clear up regression troubles the use of the set of rules regressor

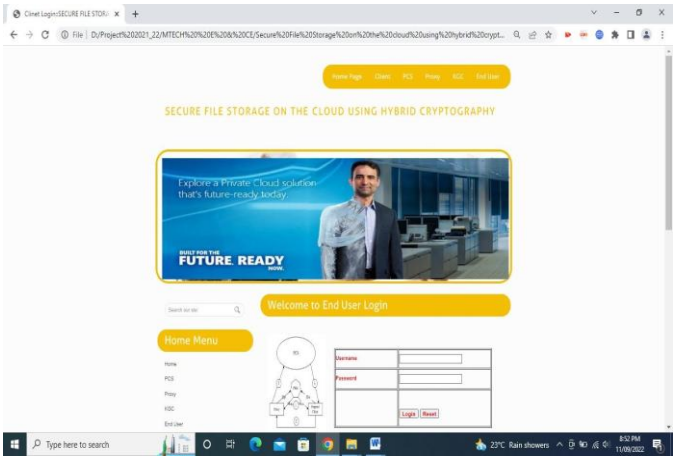
5. OUTPUT

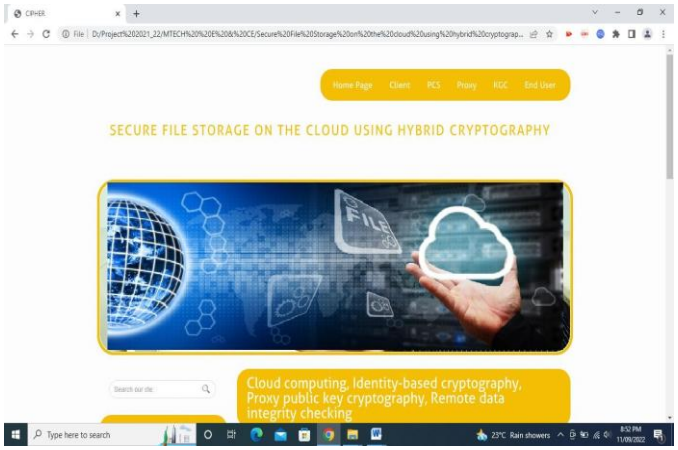












6. CODE EFFICIENCY

ACTIONS OF ENCRYPTION

The following qualities were thought to be present in this code:
Strength: A code form should make sure that just one meaning-specific code value is used to supply an object or attribute.

Extensibility: The code structure is created to support the expansion of a number of entities or attributes, giving access to the newest components of each class.

Conciseness: The code reduces the number of real-world positions needed to define and wrap each object.

Uniform size and placement: Mechanized record processing systems work particularly effectively with uniform size and format. It should no longer be possible to add prefixes and suffixes to the founding code because it violates the distinctiveness requirement.

Balance: Code that doesn't need to be updated regularly sells additional usage efficiency. The assignment of personal codes for a given entity should be done with the least possible trading possibilities both within the exact code and in the complete Coding structure.

Cost-efficient : The cost of code is having to duplicate the characteristics of the encoded entity, including the mnemonic function, to the point that either of these approaches leads to inconsistency and inflexibility.

7. CONCLUSION

Cloud Garage, which offers on-demand data set outsourcing for all types of businesses and individuals, has recently come to people's attention. Customers' lack of complete confidence in her CSP is one of the biggest and most significant barriers to its expansion, nevertheless. This is due to the fact that it can be quite challenging to assess whether a CSP complies with regulatory requirements for record preservation. Therefore, it is crucial and relevant to develop green auditing techniques to boost her owner's trust in her cloud storage. With the help of a dynamic hash desk, this article aims to establish a distinctive public verification mechanism for safe cloud storage (DHT). For the purpose of recording fact set records for dynamic verification, a DHT is a brand-new, two- dimensional information structure.

9. REFERENCES

[1]H. Dewan and R. C. Hansdah. "A Survey of Cloud Storage Fa- cilities", Proc. 7th IEEE World Congress on Services, pp. 224- 231, July 2011.

[2] C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou. "Toward Secure and Dependable Storage Services in Cloud Computing", IEEE Trans. Service Computing, vol. 5, no. 2, pp. 220- 232, 2012.

[3] K. Ren, C. Wang and Q. Wang. “Security Challenges for the Public Cloud,” IEEE Internet Computing, vol. 16, no. 1, pp. 69– 73, 2012.

[4] J. Ryoo, S. Rizvi, W. Aiken and J. Kissell. "Cloud Security Audit- ing: Challenges and Emerging Approaches", IEEE Security & Privacy, vol. 12, no. 6, pp. 68- 74, 2014.

[5] C. Wang, K. Ren, W. Lou and J. Li. "Toward Publicly Auditable Secure Cloud Data Storage Services", IEEE network, vol. 24, no. 4, pp. 19- 24, 2010.

[6] Q. Wang, C. Wang, K. Ren, W. Lou and J. Li. ‘‘Enabling Public Auditability and Data Dynamics for Storage Security inCloud Computing,’’ IEEE Trans. on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847- 859, 2011.

[7] F. Sebé, J. Domingo- Ferrer, A. Martínez- Ballesté, Y. Deswarte and J.- J. Quisquater, “Efficient Remote Data Possession Check- ing in Critical Information Infrastructures,” IEEE Trans. Knowledge Data Eng., vol. 20, no. 8, pp. 1034- 1038, 2008.

[8] A. Juels and B.S. Kaliski Jr., “PoRs: Proofs of Retrievabili ty for Large Files,” Proc. ACM Conf. Computer and Communications Se- curity (CCS ’07), pp. 584- 597, 2007.

[9] G. Ateniese, R.B. Johns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, ‘‘Provable Data Possession atUntrusted Stores,’’ Proc. 14th ACM Conf. on Comput. and Commun. Security (CCS), pp. 598- 609, 2007