Checking the Security of Data by Continuous Auditing and Providing Certificates

DurgaDevi S[1] Hemalatha D.S[2] Neranjana M[3] Mr Raja R[4]
[1,2,3]UG Scholars [4]Assistant Professor
[1,2,3,4]Department of Computer Science & Engineering
[1,2,3,4]Velammal Institute of Technology, Tiruvallur, Tamil Nadu, India

Abstract— Cloud computing has become an associate integral part of the IT infrastructure for several corporations worldwide. Security is one of the issues which reduces the growth of cloud computing and complications with data privacy and data protection. Cloud security auditing depends upon the surroundings, and also the rise of cloud computing is a crucial new context in world economics. Cloud service certificate from the cloud security alliance must have for those having a hacking background. Public cloud account compromises new attack vectors, causing 27% of organizations to have users whose accounts are potentially compromised. To prevent the file from attack, there is a need for continuous auditing and providing certificates regarding the security of the file. A file is uploaded and distributed to the cloud storage. A file is split into blocks based on Dynamic block generation algorithm. The MD5 algorithm is used to generate a signature for the particular file. Also, data gets encoded using the Base64 algorithm. Continuous auditing is done by allocating the audit time. File recovery is done by the verifier if the data gets corrupted during checking. Finally, a certificate is generated and grade is provided based on the security of the file. We also focus on the challenges and benefits of auditing the file on a cloud platform. Further on we find the advancement in the related previous technology and the gaps.

Key words: Auditing, Certification, Data Integrity, File Recovery, Security

I. INTRODUCTION

Cloud computing provides on-demand resources based on a pool of resources available by cloud providers. From the aspect of traditional computing, the advantages of cloud computing are effective cost, device independence, on-demand service, and scalability. But the security concerns are the major key aspects in the future cloud computing era. Public cloud allows for scalability that would not otherwise be possible for a single organization to achieve.

Data integrity in cloud storage is the most critical concern of cloud clients. Assurance of data integrity means data remain as it is on the server for a long time. The client cannot physically access the data from the cloud server directly, without a client's knowledge. Cloud Service Provider (CSP) can alter or delete data which are either unused by the client from a long a time or takes large memory space. Hence, there is a need for reconciliation of data periodically, for its integrity. Checking data for correction is called data integrity.

In general, an audit is when a third party, independent group is engaged to obtain evidence through inquiry, physical inspection, observation, analytic procedures, and/or re-performance. In a cloud audit, a variation of these steps are completed in order to form an opinion over the design and operational effectiveness of controls identified in the following area:

Communication, Security incidents, Network security, System development, Risk management, Data management, Vulnerability and remediation management,Tone at the top or leadership commitment to transparency and ethical behaviour.

The term certification describes the process whereby an organization, a product, or a process is tested and evaluated by an (accredited) party to determine whether or not it complies with a specific standard or a set of standards. Certificates are approved means, not only in the IT industry, to give customers fast, simple, transparent, and comparable information on protective measures implemented.

II. LITERATURE SURVEY

S.Subashini et.al[16] provides a survey of the different security risks that pose a threat to the cloud is presented. The survey is more specific to the different security issues that have emanated due to the nature of the service delivery models of a cloud computing system.

Juan Zhang et.al[17] proposes a security scheme for continuous auditing agent architecture. Provides an elliptic curve based authentication scheme that can authenticate the data source and the continuous auditing agent. After authentication, a shared key is established between the data source and the continuous auditing agent. Auditing data is protected by that shared key.

Claudio A. Ardagna et.al[15] presents a reliability certification scheme in which services are modeled as discrete-time Markov chains. A machine-readable certificate is issued to the service after validating its reliability properties, and validity of the certificate is verified using constant run-time monitoring. In addition, presents a solution that allows users to search and select services with a given set of reliability properties. The solution is integrated within existing Service-Oriented Architectures (SOA) and allows validation of users preferences both at discovery-time and at run-time.

Iryna Windhorst et.al[11] did the survey on common certification process to the increased flexibility and dynamics of cloud computing environments through using of automation potential of security controls and continuous proof of the certification status. Dynamic certification is based on a new semi-automated certification process and the continuous monitoring of critical parameters of cloud services.

R.Nithiavathy[12] considered the technique of spectrum sharing among users of service providers to share the licensed spectrum of licensed service providers. Provides a flexible distributed storage integrity auditing mechanism. The proposed design allows users or third party auditor to

audit the cloud storage with very lightweight communication and less computation cost. The auditing result ensures reliable cloud storage correctness and simultaneously achieves fast data error localization.

Kan Yang et.al[13] designed an auditing framework for cloud storage systems and propose an efficient and privacy-preserving auditing `protocol. Extends auditing protocol to support the data dynamic operations, which is efficient and provably secure in the random oracle model. Further extend auditing protocol to support batch auditing for both multiple owners and multiple clouds, without using any trusted organizer. The analysis and simulation results show that proposed auditing protocols are secure and efficient, especially it reduces the computation cost of the auditor.

Rajani Devi.T[14] provides a broad review of network security and cryptography, with particular regard to digital signatures. The purpose of a digital signature is to provide a means for an entity to bind its identity to a piece of information. The common attacks on digital signature were reviewed. The first method was the RSA signature scheme, which remains today one of the most practical and versatile techniques available. DSA and related signature schemes are two other methods reviewed. Digital signatures have many applications in information security, including authentication, data integrity, and non-repudiation was reviewed.

Gadhave Hanmant Pandurang et.al[4] introduced recovery technique is to help a user to collect information from any backup server when the server fails to provide the data to the user. There are lots of recoveries mechanisms are used to recover the data in the cloud such as HSDRT, ERGOT, LINUX BOX backup strategy. But there are some limitations in those techniques such as implementation complexity, security issues and retrieval time is high. To overcome these issues in our proposed system by using MFT [Master File Table] data storage with its index through recovery.

Praveen S.Challagidad et.al[2] relies mainly on a perception of reputation, and self-appraisal by providers of cloud services. Becoming gradually more intricate for cloud users to make a distinction with respect to trustworthiness among cloud service providers offering similar kinds of services. Proposes mainly on reputation and trust management algorithm to meet the needs.

Shivarajkumar Hiremath et.al[3] suggest an efficient public auditing technique using Third Party Auditor (TPA) to verify the integrity of data stored in the cloud. Proposed auditing scheme makes use of AES algorithm for encryption and Secure Hash Algorithm (SHA-2) algorithm to generate verification metadata or message digest for data integrity check. The analysis shows that the proposed scheme is provably secure and TPA takes constant time to audit files of different sizes.

III. PROPOSED SYSTEM

In the proposed framework, remote data integrity checking is required to verify client's information. Client will transfer document to Cloud. This document is split into blocks utilizing Dynamic Block generation Algorithm and put away in a MultiCloud domain. file Allocation Table (FAT) File System has legitimate Indexing and Metadata for the diverse Chunks of the Cloud Storage. Here the auditor consents to examine logs, which are routinely made amid checking activities by administrations suppliers to survey certification adherence. In the event that Attacker corrupts information in MultiCloud, the persistent auditing process causes the verifier to perform Block level and File level checking for remote data Integrity Checking to utilize Verifiable Data Integrity Checking Algorithm. Cloud gives arbitrary blocks to Verifier for Integrity Checking which is to shield client protection from Verifier (Third Party). file recovery is finished by the Verifier automatically if the data gets corrupted during checking. Clients can complain about the cloud for file recover.

The algorithms that has been used in our work are:

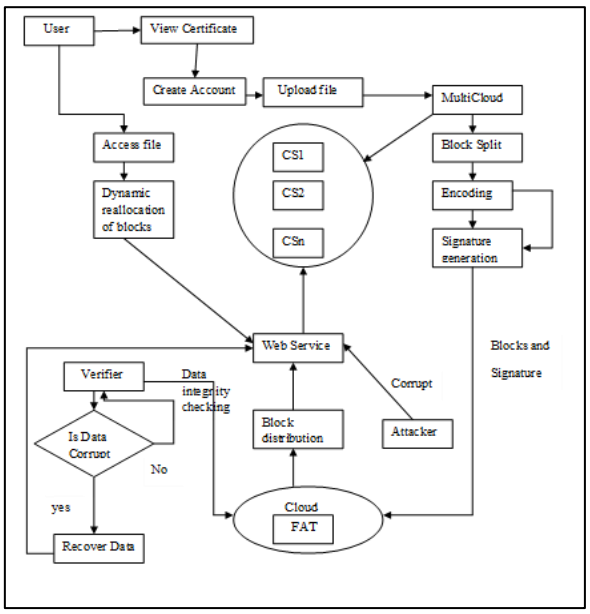
A. MD5 Algorithm:

The MD5 algorithm is a cryptographic function that accepts a message of any length as input and returns as output a fixed-length digest value to be used for authenticating the original message. The MD5 hash function was originally designed for use as a secure cryptographic for authenticating digital signatures. MD5 has been used for other than as a non-cryptographic checksum to verify data integrity and detect data corruption.Large files must be compressed before being encrypted with a private key under a public key cryptosystem such as RSA. Generally, it is used for digital signature applications.

B. BASE64 Algorithm:

Base64 encoding is a conversion of binary data to an ASCII string format. The Base64 method of encoding is used when binary data, such as images or video, is transmitted over a system. such file is transmitted in raw binary format to text-based systems. Since text-based systems interpret binary data as a wide range of characters, including special command characters. It avoids such transmission problems is to send it as plain ASCII text in Base64 encoded format.Base64 is used by MIME standard to send data except for plain text.

IV. ARCHITECTURE DIAGRAM

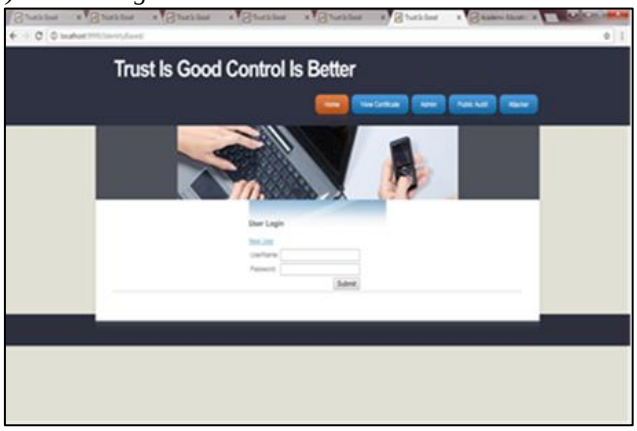


V. MODULES

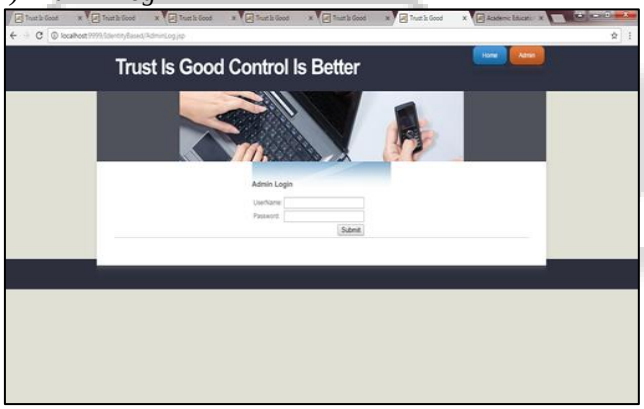
A. Enrollment

In this module, normal users who want to register in a cloud platform can get through. A user had to give their details and unique id will be created for a particular user. In the login, page user had to give their username and password. If credentials are correct then server allows to go to inside the websites or else username or password alert is generated by the server.

1) Home Page:



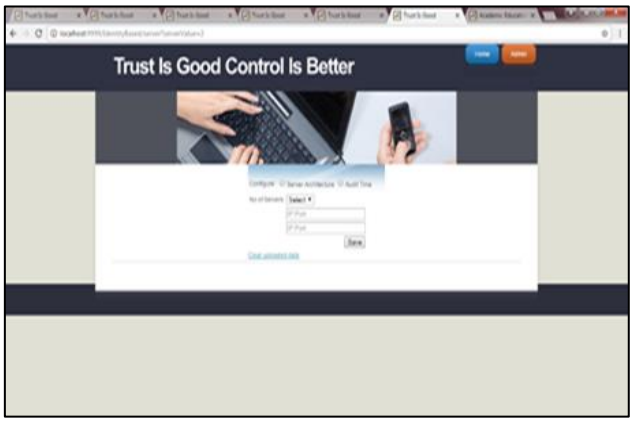
2) Admin Login



B. Server Setup

An administrator configures MultiCloud server setup. Server IP Address and Port number is given by the administrator for each Cloud. Presently a Server Architecture is made for MultiCloud Storage. On the off chance that the administrator needs to reconfigure the old MultiCloud server setup, it tends to be finished. For old server setup, FAT file can be changed or remain the same. Audit time will be set by the administrator for Data Integrity checking process.

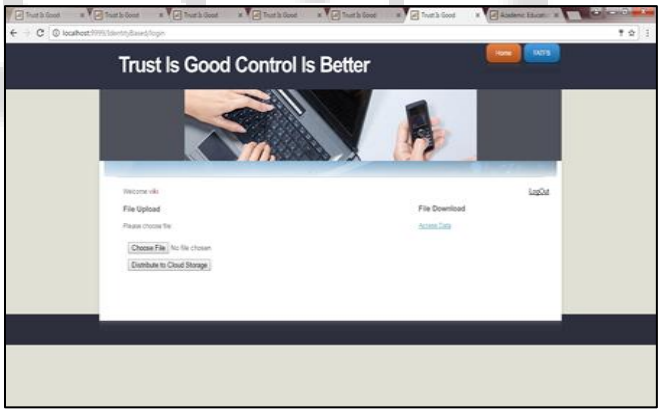
C. Configuration setup



D. Information upload and Block splitup

A client has an underlying level Registration Process at the web end. The clients give their very own data to this process. The server thus stores the data in its database. After Registration, the client can transfer documents to the server. Uploaded documents will be put away in a Server. At the point when the client transfer the information to the various cloud when it is split into various blocks utilizing dynamic block generation Algorithm and each block will be appended with Signatures before putting away the information in FATFS. The signature generated using MD5 Algorithm. Likewise the information gets encoded utilizing for Base64 Algorithm.

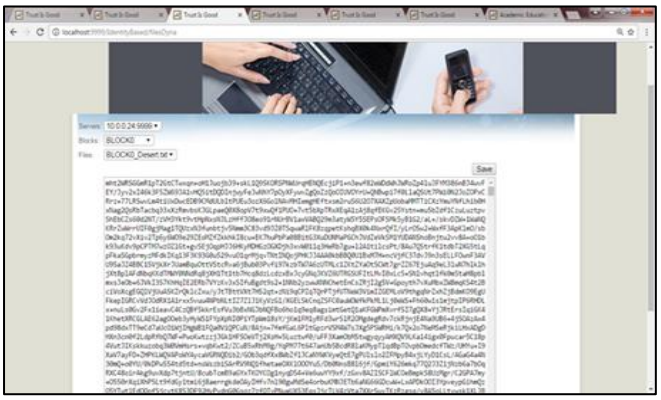
E. File Upload



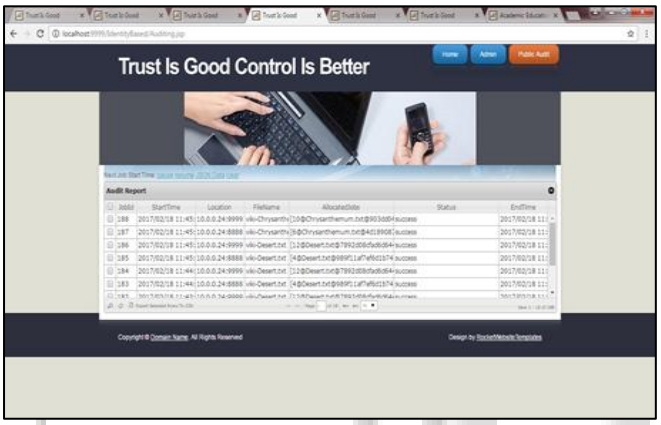
F. Data Integrity Checking

FATFS has proper Indexing and Metadata for the distinctive Chunks of the Data that is being uploaded by Client. Verifier performs Remote Integrity Checking on Cloud Data. Cloud allocates a random combination of all the blocks to the Verifier, rather than the entire document is recovered data integrity checking. This is to shield client security from an outsider (Verifier).

G. Attacker



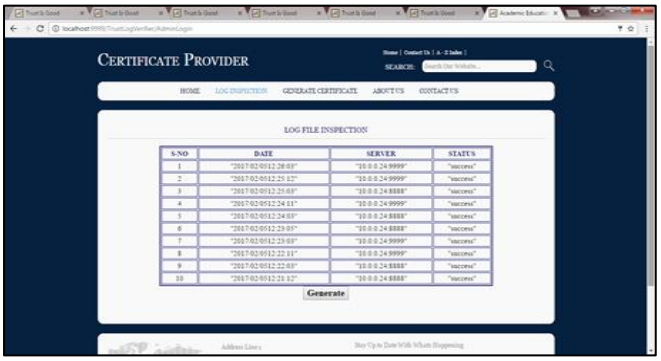
H. Audit Time and Report



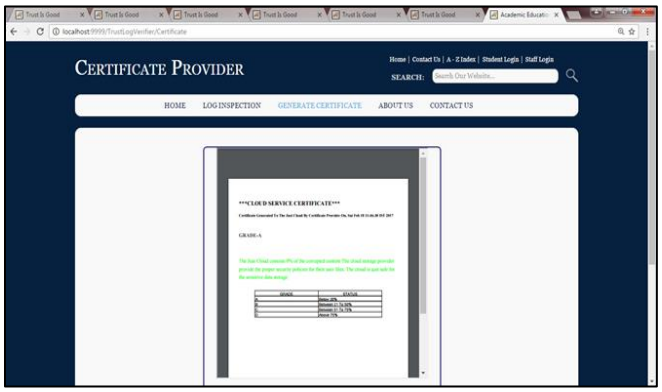
I. Document Recovery and Certificate Generation

An attacker can corrupt information in any of the cloud servers. Data Integrity Checking done by the Verifier, Verifier informs Corrupted blocks to the Cloud. Recovery Process will be finished by the verifier consequently when information gets corrupted. Client can objection to the Cloud if the client document get corrupted. Whenever a client gets to record, Blocks will be reallocated dynamically to provide access confidentiality in a cloud and FAT File System will get refreshed. An auditor will screen the cloud consistently and they give the certificate dependent on the cloud performance. When new client participates in the cloud they will read the certificate and afterward they can make an account in the cloud.

J. Log File Inspection



K. Certificate Provider



VI. CONCLUSION

Continuous auditing provides security and reliability of the file. Assigning audit time to particular file will provide consistency and cloud users can get verified with their security of data periodically. Data integrity is carried out to know about the corrupted blocks. File recovery is carried out automatically without leading to any discrepancy. The certificate is provided by the auditor based upon the security and performance of the file. As result files are secured and processed efficiently, so the cloud user can access their file on a required basis.

VII. FUTURE ENHANCEMENTS

Future research focuses on large files, such as audio, video and GIF images etc should be split into blocks and generate the signature. Time consumption is considered. Automatic Certificate Generation should be implemented so that user get periodic updates about their file.

REFERENCES

[1] Sebastian Lins, Stephan Schneider, and Ali Sunyaev, "Trust is Good, Control is Better: Creating Secure Clouds by Continuous Auditing," IEEE Transaction on Cloud Computing, vol. 6, no. 3, 2018.

[2] Challagidad, P. S., & Birje, M. N. (2017). "Trust management in cloud computing", 2017 International Conference on Smart Technologies for Smart Nation (SmartTechCon).doi:10.1109/smarttechon.2017.8358385.

[3] Hiremath, S., & Kunte, S. (2017). "A novel data auditing approach to achieve data privacy and data integrity in cloud computing,"2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT). doi:10.1109/iceeccot.2017.8284517.

[4] Pandurang, G. H., Bhimrao, C. S., & Chothe, P. (2016). "Data recovery through indexing in cloud computing", 2016 International Conference on Communication and Electronics Systems (ICCES).doi:10.1109/cesys.2016.7889921.

[5] S. Lins, P. Grochol, S. Schneider, and A. Sunyaev, "Dynamic certification of cloud services: Trust, but verify!" in Proc. IEEE Security and Privacy, vol. 14, no. 2, forthcoming, 2016.

[6] M. Becker, S. Lehrig, and S. Becker, "Systematically deriving quality metrics for cloud computing systems," in Proc. 6th ACM/SPEC Int. Conf. Perform. Eng., Austin, TX, USA, 2015, pp. 169–174.
[7] A. Pichan, M. Lazarescu, and S. T. Soh, "Cloud forensics," Digital Investigation, vol. 13, pp. 38–57, 2015.
[8] J.R. Rajalakshmi, M. Rathinraj, and M. Braveen, "Anonymizing log management process for secure logging in the cloud," in Proc. Int. Conf. Circuit, Power Comput. Technol., India, 2014, pp. 1559– 1564.
[9] M. Jans, M. Alles, and M. Vasarhelyi, "The case for process mining in auditing," Methodol. AIS Res., vol. 14, no. 1, pp. 1–20, 2013.
[10] T. Kunz, P. Niehues, and U. Waldmann, "Technische unterstut- € zung von audits bei cloud-betreibern," DuD, vol. 37, no. 8, pp. 521–525, 2013.
[11] I. Windhorst and A. Sunyaev, "Dynamic certification of cloud services," in Proc. 8th Int. Conf. Availability,eliability,Security,Regensburg,Germany, 2013, pp. 412–417.
[12] R. Nithiavathy, "Data integrity and data dynamics with secure storage service in cloud," in Proc. Int.Conf. Pattern Recog., Inform.Mobile Eng., Salem, Germany, 2013, pp. 125–130.
[13] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 9, pp. 1717–1726, Sep. 2013. Systems andNetworkTechnologies.doi:10.1109/csnt.2013.102.
[14] Devi,T. R. (2013). "Importance of Cryptography in Network Security", 2013 International Conference on Communication Systems Network Technologies. doi:10.1109/csnt.2013.102
[15] C. Ardagna, E. Damiani, R. Jhawar, and V. Piuri, "A model-based approach to reliability certification of services," in Proc. 6th IEEE Int. Conf. Digital Ecosyst. Technol., Italy, 2012, pp. 1–6.
[16] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," J. Netw. Comput. Appl.,vol. 34, no. 1, pp. 1–11, 2011.
[17] J. Zhang and C. Wan, "Securing continuous auditing in wireless network," in Proc. Int. Conf. E-Business E-Government , Shanghai,China, 2011, pp. 1–4.
[18] C.-T. Kuo, H.-M. Ruan, C.-L. Lei, and S.-J. Chen, "A mechanism on risk analysis of information security with dynamic assessment," in Proc. 3rd Int. Conf. Intell. Netw. Collaborative Syst., Fukuoka, Japan, 2011, pp. 643–646.
[19] D. Zmuda, M. Psiuk, and K. Zieli _ nski, "Dynamic monitoring framework for the SOA execution environment," Proc. Comput. Sci., pp. 125–133, 2010.
[20] Q. Fu, J.-G. Lou, Y. Wang, and J. Li, "Execution anomaly detection in distributed systems through unstructured log analysis," in Proc. Int. Conf. Data Mining, Miami, FL, USA, 2009, pp. 149–158.
[21] M. G. Alles, A. Kogan, and M. A. Vasarhelyi, "Audit automation for implementing continuous auditing," 2008.
[22] M. A. Vasarhelyi and F. B. Halper, "The continuous audit of online systems," Auditing, vol. 10, no. 1, pp. 110–125, 1991.

