DOUBLE ENCRYPTION BASED REMOTE DATA INTEGRITY CHECKING WITH PRESERVING DATA FOR CLOUD STORAGE

Dhivya A[1].,
ME Student, Department of CSE,
Dhanalakshmi Srinivasan Engineering College, Perambalur[1].
diveit.btech16@gmail.com

Mr. Raja G[2].,
Professor, Department of CSE,
Dhanalakshmi Srinivasan Engineering College, Perambalur[2]
grajathila@gmail.com

Abstract
Cloud computing is a computing technology, and the Internet has grown in current years. It can share the software program and hardware sources, and provide resources to a person's laptop or cellular device. The consumer can gain a greater efficient provider due to the fact cloud computing can combine resources From users' attitude, which includes both people and IT structures, storing data remotely into the cloud in a flexible on-demand manner brings tempting advantages such as comfort of the burden for garage control, universal data access with impartial geographical locations, and avoidance of capital expenditure on hardware, software program, and employees maintenances, and so on. To securely introduce an effective 0.33 birthday party auditor (TPA), must be able to capably audit the cloud information storage without demanding the local copy of facts, and introduce no extra on-line burden to the cloud consumer; the third birthday party auditing system should absorb no new vulnerabilities closer to user facts privacy. Public auditability implies the information owner permitting other to confirm the data owner's data is inefficient. In wellknown, the facts proprietor may also have a number of information documents that are saved in cloud garage provider. However, the statistics proprietor can not regularly verify their information because it will consume their sources which cannot manner different action. In this project, make use of and uniquely combine the public auditing protocols with double encryption method to obtain the privacy-retaining public cloud information auditing machine, which meets all integrity checking with none leakage of records. To aid green dealing with of more than one auditing duties, we in addition discover the technique of on line signature to increase our essential end result into a multi-user setting, where TPA can carry out multiple auditing obligations simultaneously. We can put in force double encryption algorithm to encrypt the statistics twice and stored cloud server.

Index Terms**:** *Cloud Framework, Public Auditing, Data Integrity Protection, Double Encryption, Multi User Setting.*

I. INTRODUCTION

Cloud computing is a computing paradigm, in which a big pool of systems are associated in private or public networks, to offer dynamically scalable infrastructure for software program, information and file storage. With the advent of this period, the charge of computation, software internet web hosting, content material garage and shipping is decreased substantially. It is a sensible technique to enjoy direct rate advantages and it has the capacity to convert a information center from a capital-extensive set up to a variable priced environment. The idea of cloud computing is primarily based mostly on a totally vital standards of reusability of IT abilities. The difference that cloud computing brings in assessment to standard ideas of "grid computing", "dispensed computing", "software computing", or "autonomic computing" is to growth horizons inside the course of organizational limitations. Forrester [1] defines cloud computing as: "A pool of abstracted, pretty scalable, and managed compute infrastructure capable of hosting prevent client programs and billed thru consumption". It is a technology that uses the net and number one some distance off servers to maintain information and packages and allows customers and corporations to use applications without installation and get entry to their personal documents at any pc with net get proper of access to. This generation allows for plenty more inexperienced computing with the aid of the use of the usage of centralizing statistics storage, processing and bandwidth. Cloud computing examples are Yahoo email, Gmail, or Hotmail. While the storage of organization statistics on some distance off servers is not a extremely-current development, current-day enlargement of cloud computing justifies a more careful take a look at its real effects associated with privateness and confidentiality troubles. As customers no longer physical own the garage in their records, traditional cryptographic primitives for the reason of records protection protection can't be straight away discovered. In particular, truely downloading all the facts for its integrity verification isn't a realistic answer because of the expensiveness in I/O and transmission rate at some stage in the community. Besides, it's miles regularly insufficient to come across the records corruption handiest while gaining access to the records, because it does not provide clients correctness guarantee for those un-accessed statistics and might be too past because of get better the records loss or damage. To absolutely make sure the records integrity and maintain the cloud customers' computation belongings in addition to on line burden, it's miles of vital significance to permit public auditing service for cloud records storage, just so clients also can motel to an

independent 0.33 birthday party auditor (TPA) to audit the outsourced information even as wished. The TPA, who has information and abilties that customers do no longer, can periodically check the integrity of all of the information saved in the cloud on behalf of the customers, which gives a much extra easier and low price way for the customers to make certain their storage correctness in the cloud. In a word, allowing public auditing services will play an essential feature for this nascent cloud monetary machine to emerge as genuinely hooked up; in which clients will need strategies to evaluate hazard and benefit bear in mind inside the cloud.The basic cloud is shown in fig 1.

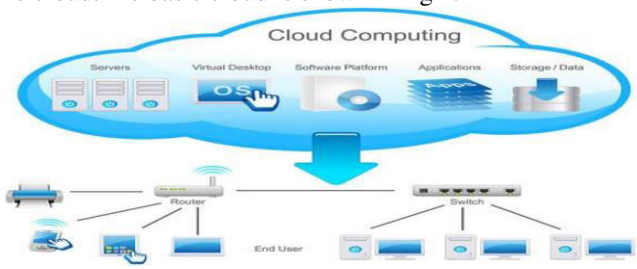

Fig 1: Cloud Deployment Model

II. RELATED WORK

G. Ateniese, et.al,…[1] provide A framework for constructing leakage-resilient ID protocols within the BRM from publicly verifiable proofs of storage (PoS) which might be computationally zero-information (ZK). PoS are interactive protocols allowing a purchaser to affirm that a server faithfully shops its record. A PoS is publicly verifiable if anyone with get entry to to the consumer's public-key can confirm the server's storage and it's far computationally ZK if, more or less speaking, its verification segment leaks no beneficial information about the document to a bounded adversary. We display how to assemble such a scheme primarily based at the RSA assumption. The secret key of the identity protocol is the encoding of a randomly-generated record and the public secret is the state information generated by using encoding the document together with the general public key for the PoS. To perceive itself, the prover executes the verification phase of the PoS with the verifier to show that it indeed holds the file. We confirmed that 0-understanding proof-of-garage schemes may be used to construct leakage-resilient identity protocols inside the bounded retrieval version (BRM). Our framework provides new insights into the BRM and unfolds new methods to construct leakage-resilient identification protocols on this version.

Z. Fu, K. Ren, et.al,…[2] provided a popular way to search over encrypted data is searchable encryption and many constructive schemes have been put forward under different applications. However, these searchable encryption schemes based on keyword no longer fully satisfy the new challenge and users' increasing needs, specifically manifested in the following two aspects. One is that most of existing schemes follow the model of "one size fits all" and ignore individual users' experience due to their different hobbies, interests or cultural backgrounds. In those schemes, the cloud will return all files that match the user's query, which may cause a huge consumption of network bandwidth. Moreover, it will cost user much time and many resources to filter his real interesting ones among a large quantity of returned files. In the practical application, different users may find different things relevant because of different importance or priorities of query terms, indicating the necessity of personalized search, which takes personal keyword preference or keyword priority into account. So how to design an efficient search scheme that can really understand the user's search intention is a pressing problem. However, these schemes cannot be directly applied in searchable encryption schemes due to the lack of consideration of privacy and security. And proposed a preferred keyword search scheme over encrypted data, but the artificial manner of measuring keyword preference has great randomness and fails to consider different users' search histories. The other one is that most of these schemes support only exact keyword search. That means the returned result is only related to the user's input. When the user queries some uncommon terms, it is possible that just a few matched results are returned and the user may be not satisfied with the returned results.

Z. Hao, S. Zhong, et.al,… [3] Analyzed the device which an increasing number of customers save their crucial information in far flung servers in the cloud, with out leaving a duplicate in their local computer systems. Sometimes the information stored within the cloud is so important that the customers have to ensure it isn't always misplaced or corrupted. While it is straightforward to check information integrity after absolutely downloading the facts to be checked, downloading huge quantities of information just for checking statistics integrity is a waste of conversation bandwidth. Hence, a number of works had been accomplished on designing remote statistics integrity checking protocols, which allow facts integrity to be checked with out completely downloading the facts. In faraway information integrity checking protocols, the consumer can mission the server about the integrity of a certain data document, and the server generates responses proving that it has get entry to to the entire and uncorrupted statistics. The simple necessities are that the customer does not want to get admission to the complete authentic facts report whilst appearing the verification of records integrity, and that the customer need to be capable of verify integrity for an infinite number of instances. Furthermore, the protocol wishes to be secure towards a malicious server that attempts to pass the facts integrity verification without access to the complete and uncorrupted information. In a realistic application, those advanced capabilities may be wanted at the equal time. For instance, don't forget an online document machine, in which the purchaser can create and regulate her documents. The client also can cooperate on a file together with her companions. When the customer or her companions modify the document, the report and the tags want to be up to date.

H. Liu, L. Chen, et.al, [4] implemented the Cloud storage is becoming increasingly popular because of a laundry list of advantages of this kind of novel storage model. Currently, many cloud storage services such as Amazon S3, Google Cloud, and Microsoft Skydrive have attracted millions of users all over the world, including individuals and organizations. The flexibility and on demand manner of cloud storage brings a lot of appealing benefits over traditional storage approach, say, relief of the burden of storage management, avoiding capital expenditure on hardware, software and personnel maintenance, access to

data with independent geographical locations. In this paper, we show the construction is not secure in their security model or in a correct security model. To be specific, with the aid of signature queries, a malicious cloud server could generate a valid response to a challenge from a third party auditor (TPA) even the server has deleted all the files of a user or has corrupted the file. Cloud servers are not necessarily fully trusted and consequently, malicious servers might discard the data that have not been or are rarely accessed for monetary reasons. As a result, strong evidence that their data accommodated on cloud keeps unchanged and is not being tampered with or partially deleted is highly essential for cloud users. Regarding the data privacy, what the scheme can achieve is that an adversary cannot recover the entire file from the auditing process, which is similar to the one wayness of encryption. In fact, the security model is unrealistic in the sense there is no a scheme that can be proven secure in this model.

J. K. Liu, et.al,… [5] analyzedend users access cloud-based applications through a web browser, thin client or mobile app while the business software and user's data are stored on servers at a remote location. The benefits of web-based cloud computing services are huge, which include the ease of accessibility, reduced costs and capital expenditures, increased operational efficiencies, scalability, flexibility and immediate time to market. Though the new paradigm of cloud computing provides great advantages, there are meanwhile also concerns about security and privacy especially for web-based cloud services. As sensitive data may be stored in the cloud for sharing purpose or convenient access; and eligible users may also access the cloud system for various applications and services, user authentication has become a critical component for any cloud system. A user is required to login before using the cloud services or accessing the sensitive data stored in the cloud. There are two problems for the traditional account/password based system. First, the traditional account/password-based authentication is not privacy-preserving. Second, it is common to share a computer among different people. It may-be easy for hackers to install some spyware to learn the login password from the web-browser.

III. EXISTING METHODOLOGIES

While cloud computing makes numerous benefits, it can be stated in bankruptcy 1 and tough safety threats in the direction of customers' outsourced records. Since cloud carrier carriers (CSP) are separate administrative entities, statistics outsourcing is clearly relinquishing person's closing control over the fate of their records. As a end result, the correctness of the facts inside the cloud is being placed at chance due to the following motives First of all, even though the infrastructures under the cloud are an awful lot extra effective and dependable than non-public computing gadgets, they may be nonetheless dealing with the wide variety of each inner and external threats for statistics integrity. Examples of outages and protection breaches of noteworthy cloud offerings appear once in a while. Second, there do exist diverse motivations for CSP to act unfaithfully towards the cloud users concerning their outsourced statistics status. CSP may reclaim garage for financial reasons by discarding statistics which have not been or are hardly ever accessed, or maybe cover records loss incidents to maintain a popularity. In brief, although outsourcing records to the cloud is economically attractive for lengthy-term huge-scale storage, it does no longer right away provide any assure on facts integrity and availability. This trouble, if not well addressed, may impede the achievement of cloud architecture. As customers now not physically own the storage in their information, conventional cryptographic primitives for the purpose of data security protection cannot be directly adopted. In precise, without a doubt downloading all the facts for its integrity verification isn't a practical solution due to the expensiveness in I/O and transmission value throughout the community. Besides, it's miles often insufficient to locate the statistics corruption only whilst having access to the statistics, as it does now not provide customers [2] correctness assurance for the ones un-accessed information and is probably too overdue to recover the records loss or harm.

3.1. WATERMARKING SCHEME

And put into effect the system to provide water marking technique, to keep the records or images within the cloud server by using assigning the public key, and this key and watermarking images are sent to 1/3 party and 0.33 birthday party have complete authority to check the important thing and sent it to the server, and there Third Party Auditor must have a public key each time the information to be retrieved. In the watermarking procedure, the safety stage may be very excessive so the statistics or pictures can not be diagnosed by means of the attackers in the cloud and also use Compression approach for watermark photo to reduce verbal exchange overhead. The main factors in watermarking procedure: an embedded, a verbal exchange channel and a detector. Watermark statistics is embedded into original image itself, and it's miles completed in the encryption system for making security on authentic statistics. Embedded is similar to encryption technique that is used to exchange content into every other format with the help of the name of the game key. Detector process is likewise just like decryption method that is used to perform reverse procedure of encryption. The watermark information is embedded inside the authentic picture earlier than the watermarked photograph is transmitted over the conversation channel, in order that the watermark image may be detected at the receiving give up.

3.2 ONE RING TO RULE THEM ALL (ORUTA) scheme:

Then implemented ORUTA that consist of a privacy maintaining public auditing mechanism for shared statistics in an untrusted cloud. In Oruta, employ ring signatures to construct homomorphic authenticators, in order that the 1/3 birthday celebration auditor is capable of confirm the integrity of shared facts for a fixed of customers without retrieving the entire data — while the identity of the signer on each block in shared facts is stored personal from the TPA. In addition, extend the mechanism to help batch auditing, which can audit more than one shared data concurrently in a single auditing venture. Meanwhile, Oruta keeps to use random masking to useful resource data privateness inside the route of public auditing, and leverage index hash tables to help fully dynamic operations on shared

data. A dynamic operation shows an insert, delete or update operation on a single block in shared facts. In this paper, we best recollect the way to audit the integrity of shared statistics in the cloud with static agencies. It way the group is pre-described earlier than shared facts is created in the cloud and the membership of clients in the organization is not changed in some unspecified time in the future of statistics sharing. The real character is answerable for determining who is capable of percentage her statistics earlier than outsourcing statistics to the cloud. Another thrilling hassle is a way to audit the integrity of shared facts within the cloud with dynamic organizations — a new user can be introduced into the group and an present employer member can be revoked in the path of statistics sharing — while despite the fact that preserving identification privateness.

IV. PROPOSED METHODS

The Machine version on this project involves 3 parties: the cloud server, a set of customers and a public verifier. There are forms of customers in a set: the authentic person and some of institution users. The authentic user first of all creates shared records in the cloud, and stocks it with institution users. Both the unique person and institution customers are individuals of the organization. Every member of the organization is allowed to access and adjust shared information. Shared facts and its verification metadata (i.E. Signatures) are each saved inside the cloud server. A public verifier, which include a 3rd-birthday party auditor (TPA) offering professional information auditing offerings or a records user outside the institution proceeding to make use of shared facts, is able to publicly affirm the integrity of shared information stored inside the cloud server. When a public verifier wishes to check the integrity of shared data, it first sends an auditing project to the cloud server. After receiving the auditing undertaking, the cloud server responds to the public verifier with an auditing evidence of the possession of shared information. Then, this public verifier assessments the correctness of the complete statistics by means of verifying the correctness of the auditing proof. Essentially, the manner of public auditing is a assignment and-reaction protocol among a public verifier and the cloud server.

Public Auditing A public verifier is able to publicly affirm the integrity of shared information with out retrieving the entire information from the cloud.

Correctness A public verifier is ready to properly verify shared information integrity.

Unforgetability Only a person in the group can generate valid verification metadata (i.e., signatures) on shared facts.

Identity Privacy A public verifier can't distinguish the identity of the signer on each block in shared records all through the technique of auditing.

With cloud computing and storage, users are able to access and to share sources provided with the aid of cloud provider companies at a lower marginal price. It is ordinary for users to leverage cloud garage offerings to share data with others in a set, as data sharing becomes fashionable feature in maximum cloud garage services, which includes Drop box, i-Cloud and Google Drive. The integrity of information in cloud storage, however, is challenge to skepticism and scrutiny, as information stored within the cloud can effortlessly be lost or corrupted because of the inevitable hardware/software disasters and human mistakes. The traditional method for checking statistics correctness is to retrieve the entire records from the cloud, after which verify records integrity with the aid of checking the correctness of signatures or hash values of the complete records. Certainly, this traditional approach able to efficaciously test the correctness of cloud information. However, the efficiency of using this conventional method on cloud statistics is in doubt. The essential reason is that the dimensions of cloud records is huge in general. Downloading the whole cloud records to verify information integrity will fee or even waste consumer's amounts of computation and communique resources, particularly while information had been corrupted in the cloud. Recently, many mechanisms were proposed to allow now not only a facts proprietor itself however also a public verifier to successfully carry out integrity checking without downloading the entire data from the cloud, that is referred to as public auditing. In those mechanisms, statistics is divided into many small blocks, in which every block is independently signed by using the owner; and a random combination of all the blocks instead of the whole facts is retrieved during integrity checking. A public verifier may be a facts user (e.G. Researcher) who would love to utilize the owner's statistics thru the cloud or a 3rd-birthday party auditor (TPA) who can provide professional integrity checking service. In this proposed machine we are able to enforce Merkle Hash Tree to spilt the documents into diverse elements and to provide double encryption concept to encrypt the data first at proprietor facet and again encrypt the records based totally on TPA supplied keys. Finally offer batch auditing schemes to perform multiple obligations at a time and user stage privacy can be implemented to proportion the data without any leakages. The proposed framework is shown in fig 2.

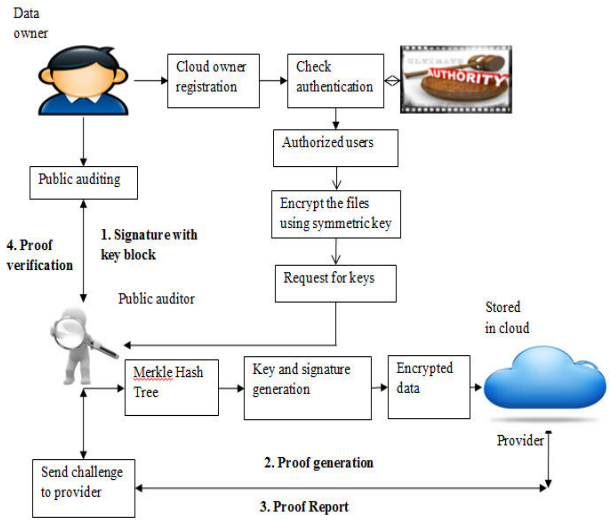

Fig 2. Proposed Framework

V. CONCLUSION

Cloud computing securities are mentioned and analyzed in previous study. In this venture, some of the

privateness threats are addressed and the strategies to triumph over them are surveyed. While some tactics applied traditional cryptographic methods to achieve privacy, some other tactics stored them away and focused on trade methodologies in attaining privateness. Also, procedures to hold privacy at the time of public auditing are also discussed. Thus, to conclude it's far necessary that each cloud user must be assured that his facts is saved, processed, accessed and audited in a secured manner at any time. Data freshness is vital to protect against misconfiguration mistakes or rollbacks brought about deliberately and can increase an authenticated document device that helps the migration of an enterprise-magnificence dispensed file device into the cloud efficaciously, transparently and in a scalable manner. It's authenticated within the experience that allows an business enterprise tenant to verify the freshness of retrieved facts whilst acting the record device operations. The person must be given whole get admission to manage over the posted records. Also, effective protection mechanisms should always supplement every cloud software. Attaining a lot of these would come to be in reaching the lengthy dreamt imaginative and prescient of secured Cloud Computing in the nearest destiny.

REFERENCES

[1] G. Ateniese, A. Faonio, and S. Kamara, "Leakage-resilient identification schemes from zero-knowledge proofs of storage," in IMA Inte. Conf. Cryptography and Coding, 2015, pp. 311–328.

[2] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," IEEE Trans. Parallel Distrib.Syst., doi.10.1109/TPDS. 2015.2506573.

[3] Z. Hao, S. Zhong, and N. Yu, "A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability," IEEE Trans. Knowl.Data Eng., vol.23, no.9, pp.1432-1437, 2011.

[4] H. Liu, L. Chen, Z. Davar, and M. Pour, "Insecurity of an efficient privacy-preserving public auditing scheme for cloud data storage," J. Universal Comput.Sci., vol. 21, no. 3, pp. 473–482, 2015.

[5] J. K. Liu, M. H. Au, X. Huang, R. Lu, and J. Li, "Fine-grained twofactor access control for web-Based cloud computing services," IEEE Trans. Inf. Forens. Security, vol. 11, no. 3, pp. 484–497, 2016.

[6] F. Seb´e, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and J. J. Quisquater, "Efficient remote data possession checking in critical information infrastructures," IEEE Trans. Knowl. Data Eng., vol. 20, no.8, pp. 1034–1038, 2008

[7] C. Wang, Q. Wang, S. C, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," IEEE Trans. Comput., vol. 62, no. 2, pp. 362–375, 2013.

[8] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Proc. IEEE Int. Conf. Comput.Commun. (INFOCOM), 2010, pp. 1–9.

[9] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 2, pp. 340-352, 2015.

[10] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and Z. Dong, "Round-efficient and sender-unrestricted dynamic group key agreement protocol for secure group communications," IEEE Trans. Inf. Forens.Security, vol. 10, no. 11, pp. 2352-2364, 2015.