International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307 OPEN ACCESS

Available Online at : www.ijsrcseit.com

doi : https://doi.org/10.32628/IJSRCSEIT

Cloud Based Third Party Storage Auditing Service

Md Tarique Khan[1], Prof. Mashhood Siddiqui[2]

[1]Department of Computer Science and Engineering, Bhabha Engineering Research Institute, Bhopal, India

[2]Assistant Professor, Department of Computer Science and Engineering, Bhabha Engineering Research Institute, Bhopal, India

ARTICLEINFO

Article History:

Accepted: 01 Oct 2023

Published: 20 Oct 2023

Publication Issue

Volume 9, Issue 5

September-October-2023

Page Number

298-311

ABSTRACT

To completely make certain the statistics protection and store the cloud users' computation assets, it's miles of essential significance to permit public audit capacity for cloud records storage so that the customers can also hotel to a 3rd Party auditor (TPA), who has the understanding and abilities that the customers do now not, to audit the outsourced facts whilst wished. Based on the audit end result, TPA could launch an audit file, which would no longer handiest assist customers to assess the risk in their subscribed cloud facts offerings, however additionally be useful to the cloud service company to improve their cloud primarily based service platform. In a phrase, allowing public chance auditing protocols will play an essential function in this nascent cloud economic system to come to be fully hooked up; wherein users will want ways to assess risk and gain agree with within the Cloud. In this paper, a survey has been carried out for third birthday party audit offerings and hassle statement has been given in the paper based totally on current techniques.

Keywords : Third Party, Auditing, Cloud Computing, Encryption Algorithms, Storage Security.

I. INTRODUCTION

Cloud Computing has been envisioned as the next era architecture of IT agency, due to its long list of remarkable advantages in the IT records: on-demand self-provider, ubiquitous community get entry to, place impartial resource pooling, speedy useful resource elasticity, usage-primarily based pricing and transference of danger [1]. As a disruptive generation with profound implications, Cloud Computing is transforming the very nature of the way corporations use information generation. One fundamental thing of this paradigm moving is that facts is being centralized or outsourced into the Cloud. From the consumer's angle, along with both individuals and IT enterprises, storing information remotely into the cloud in a flexible on-call for manner brings appealing benefits: comfort of the weight for garage control, prevalent facts get admission to to independent geographical locations, and avoidance of capital expenditure on hardware, software, and employees maintenances, etc. [2].

While Cloud Computing makes these advantages more attractive than ever, it additionally brings new and hard safety threats towards users' outsourced facts. Since cloud service carriers (CSP) are separate administrative entities, records outsourcing is in reality relinquishing person's ultimate control over the destiny of their statistics. As a end result, the correctness of the information within the cloud are being positioned at hazard because of the subsequent reasons. First of all, despite the fact that the infrastructures underneath the cloud are much extra effective and reliable than non-public computing gadgets, they may be nevertheless going through the wide variety of both internal and outside threats for statistics integrity. Examples of outages and security breaches of noteworthy cloud offerings seem from time to time [3]–[5].

Secondly, for the blessings of their own, there do exist various motivations for cloud provider providers to behave unfaithfully in the direction of the cloud customers concerning the status in their outsourced information. Examples consist of cloud carrier companies, for monetary motives, reclaiming storage by discarding data which have no longer been or is hardly ever accessed, or even hiding statistics loss incidents if you want to keep a recognition [6]–[8]. In brief, even though outsourcing information into the cloud is economically attractive for the cost and complexity of long-time period huge-scale statistics storage, it does now not offer any assure on facts integrity and availability. This problem, if not nicely addressed, may also hinder the a hit deployment of the cloud architecture. As users not bodily own the garage in their statistics, conventional cryptographic primitives for the reason of records protection safety can not be at once followed. Thus, how correctly confirm the correctness of outsourced cloud statistics with out the local reproduction of statistics documents will become a huge challenge for facts storage security in Cloud Computing. Note that truely downloading the information for its integrity verification isn't always a sensible solution due to the expensiveness in I/O fee and transmitting the document throughout the community. Besides, it's miles frequently inadequate to detect the information corruption when gaining access to the facts, because it is probably too late to get better the data loss or harm. Considering the large length of the outsourced records and the user's limited useful resource functionality, the potential to audit the correctness of the data in a cloud surroundings may be bold and steeply-priced for the cloud users [8], [9].

Therefore, to completely make certain the statistics safety and keep the cloud customers' computation resources, it's far of vital significance to enable public audit potential for cloud information storage so that the users might also hotel to a third party auditor (TPA), who has understanding and abilties that the customers do not, to audit the outsourced data while wanted. Based on the audit end result, TPA may want to release an audit record, which would now not handiest assist users to evaluate the chance of their subscribed cloud information offerings, however also be beneficial to the cloud carrier provider to enhance their cloud based totally carrier platform [7]. In a word, allowing public risk auditing protocols will play an crucial role on this nascent cloud economic system to grow to be absolutely mounted; in which users will want approaches to evaluate chance and advantage agree with in Cloud. Recently, the belief of public audit ability has been proposed within the context of ensuring remotely saved facts integrity beneath one-of-a-kind structures and protection fashions [6], [8], [10], [11]. Public audit ability permits an outside celebration, similarly to the person himself, to confirm the correctness of remotely stored data. However, maximum of those schemes [6], [8], [10] do no longer aid the privacy safety of customers' information towards external auditors, i.E., they will probably reveal user statistics records to the auditors, as can be mentioned in Section III-C. This extreme disadvantage significantly influences the security of those protocols in Cloud Computing. From the angle of protective information privacy, the customers, who personal the information and rely upon TPA only for the storage

protection of their facts, do not need this auditing system introducing new vulnerabilities of unauthorized information leakage towards their records security [12]. Moreover, there are prison regulations, along with the United States Health Insurance Portability and Accountability Act (HIPAA) [13], further stressful the outsourced facts not to be leaked to external events [7]. Exploiting information encryption before outsourcing [11] is one way to mitigate this privacy difficulty, but it's miles only complementary to the privacy-retaining public auditing scheme to be proposed on this paper. Without a nicely designed auditing protocol, encryption itself cannot save you information from "flowing away" toward external events all through the auditing procedure.

Thus, it does now not completely clear up the problem of protecting facts privateness however just reduces it to the one of managing the encryption keys. Unauthorized facts leakage nevertheless remains a hassle because of the capacity publicity of encryption keys. Therefore, a way to allow a privateness-retaining 1/3-party auditing protocol, independent to information encryption, is the hassle we're going to address on this paper. Our paintings is many of the first few ones to help privacy-retaining public auditing in Cloud Computing, with a focus on information garage. Besides, with the superiority of Cloud Computing, a foreseeable increase of auditing duties from unique customers may be delegated to TPA.

II. RELATED WORK

Definitions and Framework

We observe a similar definition of previously proposed schemes in the context of remote records integrity checking [9], [11], [13] and adapt the framework for our privacy-retaining public auditing device. A public auditing scheme consists of four algorithms (KeyGen, SigGen, GenProof, VerifyProof). KeyGen is a key era set of rules this is run by the user to setup the scheme. SigGen is utilized by the person to generate verification metadata, which may also include digital signatures. GenProof is run by means of the cloud server to generate a proof of records garage correctness, while VerifyProof is run by using the TPA to audit the evidence. Running a public auditing device includes stages, Setup and Audit:

Setup

The consumer initializes the public and secret parameters of the device by way of executing KeyGen, and pre-strategies the records file F by way of using SigGen to generate the verification metadata. The person then stores the information report F and the verification metadata on the cloud server, and delete its neighborhood reproduction. As a part of pre-processing, the user may also adjust the information document F by expanding it or such as additional metadata to be stored at server.

Audit

The TPA issues an audit message or venture to the cloud server to make certain that the cloud server has retained the facts document F well on the time of the audit. The cloud server will derive a response message by way of executing GenProof the use of F and its verification metadata as inputs. The TPA then verifies the response through Verify Proof. Our framework assumes the TPA is stateless, i.E., TPA does no longer want to hold and update state among audits, that is a perfect belongings specially in the public auditing machine [13]. Note that it is simple to extend the framework above to capture a stateful auditing device, essentially by splitting the verification metadata into parts that are saved by the TPA and the cloud server respectively. Our design does not anticipate any extra assets on the information document. If the user wants to have greater mistakes-resilience, he can first redundantly encodes the information file after which uses our device with the information that has blunders-correcting codes integrated.

The Basic Schemes

Before giving our primary result, we examine classes of schemes as a heat-up. The first one is a MAC-primarily

based solution which suffers from unwanted systematic demerits bounded utilization and stateful verification, which may pose an extra online burden to customers, in a public auditing placing. This also indicates that the auditing hassle is still no longer clean to solve even supposing we have introduced a TPA. The second one is a gadget primarily based on homomorphic linear authenticators (HLA), which covers a whole lot recent proof of garage systems. We will pinpoint the motive why all current HLA-based systems are not privateness retaining. The evaluation of these simple schemes ends in our predominant result, which overcomes a lot of these drawbacks. Our major scheme to be supplied is based totally on an implementation of ECC on a cloud.

MAC-based Solution

There are two viable approaches to utilize MAC to authenticate the information. A trivial manner is just uploading the facts blocks with their MACs to the server, and sends the corresponding secret key sk to the TPA. Later, the TPA can randomly retrieve blocks with their MACs and check the correctness thru sk. Apart from the high (linear in the sampled records size) conversation and computation complexities, the TPA requires the information of the statistics blocks for verification. To dodge the requirement of the data in TPA verification, one may also limit the verification to just encompass equality checking. However, it suffers from the following severe drawbacks:

1) The wide variety of times a selected records file may be audited is restricted by means of the wide variety of mystery keys that have to be constant a priori. Once all viable secret keys are exhausted, the user then has to retrieve records in full to re-compute and re-submit new MACs to TPA;

2) The TPA also has to keep and replace nation among audits, i.E., maintain tune on the found out MAC keys. Considering the probably big number of audit delegations from multiple customers, keeping such states for TPA may be difficult and blunders prone;

3) it could simplest support static statistics, and can't successfully address dynamic facts in any respect. However, assisting facts dynamics is likewise of vital importance for cloud storage structures. For the motive of brevity and clarity, our foremost protocol may be supplied primarily based on static facts.

HLA-based Solution

To efficiently guide public auditability while not having to retrieve the records blocks themselves, the HLA technique [9], [13], [8] can be used. HLAs, like MACs, are also some unforgivable verification metadata that authenticates the integrity of a facts block. The distinction is that HLAs can be aggregated. It is viable to compute an aggregated HLA, which authenticates a linear combination of the individual records blocks.

Overview of Privacy-Preserving Public Auditing Scheme

To achieve privateness-keeping public auditing, we advocate to uniquely combine the homomorphic linear authenticator with random protecting method. In our protocol, the linear combination of sampled blocks inside the server's reaction is masked with randomly generated by means of the server. With random masking, the TPA now not has all the vital data to accumulate a accurate organization of linear equations and consequently can't derive the person's statistics content, regardless of what number of linear mixtures of the same set of document blocks may be gathered. On the alternative hand, the ideal validation of the block-authenticator pairs can nevertheless be performed in a brand new way with a purpose to be proven rapidly, even with the presence of the randomness. Our layout uses a public key based ECDHA, to equip the auditing protocol with public auditability. Specifically, we use the ECC proposed in [2], that's based on the quick signature scheme.

Support for Data Dynamics

In Cloud Computing, outsourced statistics may not handiest be accessed but additionally up to date frequently by customers for various software functions [21], [8], [22], [23]. Hence, supporting information dynamics for privacy-preserving public auditing is also

of paramount importance. Now we display a way to construct upon the existing work [8] and adapt our essential scheme to assist data dynamics, which include block stage operations of modification, deletion and insertion.

Generalization

As cited before, our protocol is based totally on the ECC]. One may practice the random covering method we used to construct the corresponding zero understanding evidence for exclusive homomorphic identification protocols. Therefore, our privacy-preserving public auditing gadget for comfortable cloud garage may be generalized based totally on different complexity assumptions, along with factoring [25].

Digital Signature

The Digital signature scheme is designed to provide the virtual counterpart to handwritten signatures A virtual signature is quite a number depending on a few secret known only to the signer (the signer's personal key), and, additionally, on the contents of the message being signed. Signatures need to be verifiable -- if a dispute arises as to whether or not an entity signed a report, an impartial third birthday celebration have to be able to remedy the matter equitably, without requiring get admission to to the signer's private key. An utility generates a virtual signature for a message through first applying a hash of the message to the digital signature generates callable provider. For imposing the virtual signatures will use the Hash Algorithm called SHA1.

3.8.1 SHA-1:

A hash function is actually an set of rules that takes a string of any duration and reduces it to a unique fixed period string. Hashes are used to make sure statistics and message integrity, password validity as well as the premise of many other cryptographic systems. The SHA-1 is known as a one-way hash characteristic, that means there may be no regarded mathematical technique of computing the input given simplest the output. The specification of the SHA-1, as defined with the aid of Federal Information Processing Standards (FIPS) Publication a hundred and eighty-2, states that the input consists of 512 bit blocks with a complete input period less than 264 bits. Inputs which do no longer agree to integer multiples of 512 bit blocks are padded earlier than any block is an enter to the hash characteristic. The SHA-1 set of rules outputs a hundred and sixty bits, known as the digest. The full SHA-1 specification A hash isn't 'encryption' – it can't be decrypted back to the unique text (it is a 'one-manner' cryptographic feature, and is a set length for any length of supply textual content). This makes it suitable when it's miles appropriate to compare 'hashed' versions of texts, rather than decrypting the text to obtain the unique model. Such applications encompass storing passwords, assignment handshake authentication, and virtual signatures.

To validate a password,-you could shop a hash of the password, then when while the password is to be authenticated, you hash the password the consumer materials, and if the hashed variations fit, the password is authenticated; however the authentic password can not be obtained from the stored hash Challenge handshake authentication (or 'challenge hash authentication') avoids transmissions passwords in 'clear' – a consumer can send the hash of a password over the net for validation via a server without threat of the unique password being intercepted.

Anti-tamper – link a hash of a message to the unique, and the recipient can re-hash the message and compare it to the provided hash: if they suit, the message is unchanged; this may additionally be used to verify no information-loss in transmission.

Digital signatures are instead more involved, however in essence, you could sign the hash of a document by encrypting it together with your non-public key, generating a digital signature for the record. Anyone else can then test that you authenticated the text through decrypting the signature with your public key to gain the original hash again, and evaluating it with their hash of the textual content.

III. METHODOLOGY

Problem Statement

The System and Threat Model

We consider a cloud data storage service involving three different entities, as illustrated in Fig. 1:

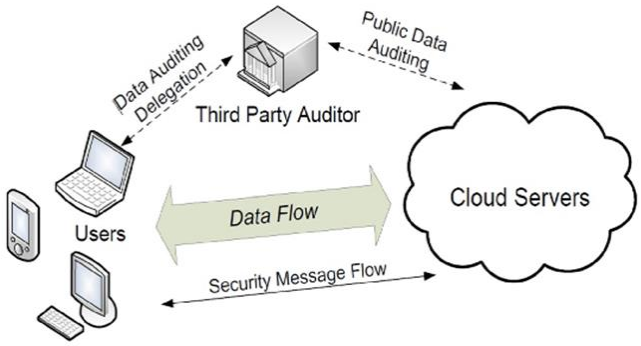


Fig 1: The architecture of cloud data storage service

The cloud consumer, who has big quantity of statistics documents to be stored in the cloud; the cloud server (CS), that is managed with the aid of the cloud carrier company (CSP) to provide facts garage service and has considerable storage space and computation resources (we can not differentiate CS and CSP hereafter); the third birthday celebration auditor (TPA), who has knowledge and talents that cloud customers do no longer have and is trusted to assess the cloud garage carrier reliability on behalf of the consumer upon request. Users rely upon the CS for cloud statistics garage and preservation. They can also dynamically have interaction with the CS to access and replace their stored information for diverse application functions.

As customers now not own their statistics domestically, it's far of vital importance for users to make sure that their statistics are being effectively saved and maintained. To store the computation aid as well as the net burden doubtlessly delivered by way of the periodic garage correctness verification, cloud users may also inn to TPA for ensuring the storage integrity of their outsourced records, at the same time as hoping to keep their statistics non-public from TPA. We anticipate the records integrity threats toward customers' records can come from each inner and outside attacks at CS. These might also include: software insects, hardware disasters, bugs in the community route, economically motivated hackers, malicious or accidental control mistakes, and so forth. Besides, CS can be self-involved. For their personal benefits, along with to keep recognition, CS would possibly even determine to cover these facts corruption incidents to customers. Using 0.33-celebration auditing provider gives a fee-effective method for users to gain agree with in Cloud. We assume the TPA, who is inside the enterprise of auditing, is dependable and impartial. However, it may harm the consumer if the TPA may want to examine the outsourced records after the audit. Note that during our model, beyond users' reluctance to leak facts to TPA, we also count on that cloud servers has no incentives to expose their hosted records to outside parties. On the only hand, there are policies, e.G. HIPAA [16], inquiring for CS to keep customers' facts privateness. On the opposite hand, as users' records belong to their enterprise asset [10], there also exist economic incentives for CS to defend it from any outside parties. Therefore, we expect that neither CS nor TPA has motivations to collude with every other at some stage in the auditing manner. In different phrases, neither entities will deviate from the prescribed protocol execution in the following presentation. To authorize the CS to respond to the audit delegated to TPA's, the consumer can problem a certificates on TPA's public key, and all audits from the TPA are authenticated against this sort of certificate. These authentication handshakes are left out inside the following presentation.

Design Goals

To enable privacy-preserving public auditing for cloud data storage under the aforementioned model, our protocol design should achieve the following security and performance guarantees.

- Public auditability: To permit TPA to verify the correctness of the cloud information on call for with out retrieving a copy of the whole

information or introducing additional on line burden to the cloud users.

- Storage correctness: To make sure that there exists no cheating cloud server that could pass the TPA's audit without indeed storing users' statistics intact.
- Privacy-preserving: To ensure that the TPA can not derive customers' statistics content material from the statistics accumulated during the auditing manner.
- Batch auditing: To allow TPA with comfortable and green auditing capability to cope with multiple auditing delegations from in all likelihood large wide variety of various users concurrently.
- Lightweight: To permit TPA to perform auditing with minimal communique and computation overhead.
- Cloud Computing Benefits: Cost including decrease implementation and renovation cost. Less hardware to buy and guide. Flexible and Agile computing Platform. Highly Scalable. High Performance useful resource. High Reliability. Cloud computing enables corporations to lessen electricity, cooling, garage and area usage. Better IT Resource control and Business Focus. Rapid Development, Deployment and trade management. Better Performance. Improved Security.
- Architecture of Cloud Computing: NIST (National Institute of Standards and Technology) is a properly familiar group everywhere in the international for his or her paintings within the area of Information Technology. NIST defines the Cloud Computing structure by describing five essential traits, three cloud services fashions and four cloud deployment fashions As defined above, there are five important characteristics of Cloud Computing which explains there relation and distinction from the traditional computing.
- On-demand-self-service: Consumer can provision or un-provision the offerings while needed, without the human interplay with the provider issuer.
- Broad Network Access: It has capabilities over the network and accessed through standard mechanism.
- Resource Pooling: The computing sources of the company are pooled to serve a couple of customers which might be the usage of a multi-tenant model, with diverse physical and digital resources dynamically assigned, relying on purchaser call for.
- Rapid Elasticity: Services can be rapidly and elastically provisioned.
- Measured Service: Cloud computing systems routinely control and optimize resource usage by using offering a metering functionality to the sort of services.

Hardware Layer:

This layer is chargeable for handling the bodily sources of the cloud, which include physical servers, routers, switches, energy and cooling structures. In practice, the hardware layer is usually carried out in statistics facilities.

Infrastructure Layer:

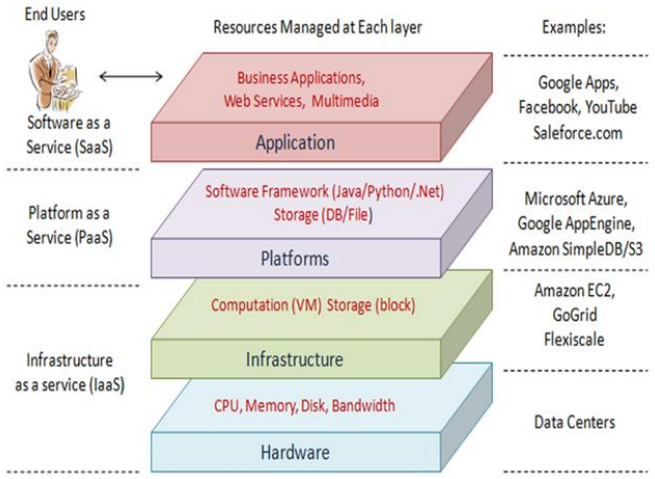
Also known as the virtualization layer, the infrastructure layer creates a pool of garage and computing assets by partitioning the physical aid the use of virtualization technologies. The infrastructure layer is an critical issue of cloud computing, considering that many key capabilities, along with dynamic resource task, are best made to be had through virtualization technology.

Platform Layer:

Built on pinnacle of the infrastructure layer, the platform layer includes working systems and application frameworks. The cause of the platform layer is to limit the burden of deploying programs without delay into VM boxes.

Application Layer:

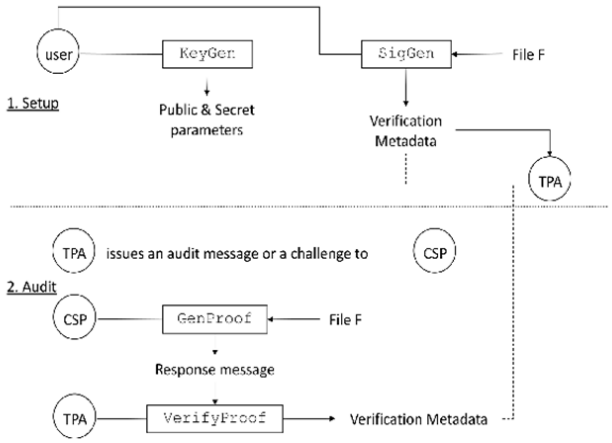
The application layer consists of the actual cloud applications.



The research offers with the growing an software by using the usage of gathering and analyzing the facts of the department, then that software ought to be deployed at the cloud. Only the legal clients can be capable of get admission to the statistics at the cloud. In order to get the information at the cloud the patron used to first login after you have got the authorization he can be capable of get admission to the records .The systems are associated with the Internet and simplest that credentials will gets the accessibility. Security also plays an essential function. Cloud computing moves the software software program application and databases to the huge statistics centers, wherein the management of the facts and services won't be surely straightforward. This precise characteristic, but, will increase many new safety challenges which have now not been well understood. Data Security worries arising due to the reality every client records and software are dwelling on Provider Premises[6].Clouds generally have a safety shape, but have many customers with unique needs this hassle of Security can be lessen to a point by using way of encrypting the records with the useful resource of using encryption algorithms. Clouds are massively complicated structures may be reduced to easy primitives which may be replicated lots of instances and commonplace purposeful gadgets, These complexities create many problems associated with protection in addition to all elements of Cloud computing. There are 3 sorts of statistics in cloud computing, i.E. Storage, Transmission and processing each of the type has its very own Encryption Algorithm for keeping the security. Amongs the unique sorts of Encryption Algorithm we're the usage of an ECC Algorithm as benchmark Algorithm which we have been applied inside the protection of the software. In this Algorithm we centered specifically on four protection parameters which incorporates Authentication, Encryption, separation of obligations and Integrity. Four roles are supplied in the Application i.E. Admin, TPA, Staff and Student and hence each characteristic has their own privileges as constant with the function and the Data it truly is being traveled for the duration of the transmission is encrypted by the use of the ECC Algorithm for the relaxed transmission of statistics.

Software Architecture

Our software describes in two main modules Setup and Audit as mentioned in fig 3:



The user initializes the public and mystery parameters of the gadget by executing KeyGen, and pre-procedures the facts file F by means of the usage of SigGen to generate the verification metadata. The consumer then shops the records file F and the verification metadata on the cloud server, and deletes its nearby copy. As part of pre-processing, the person may additionally alter the information document F by using expanding it or which include additional metadata to be stored on the server.

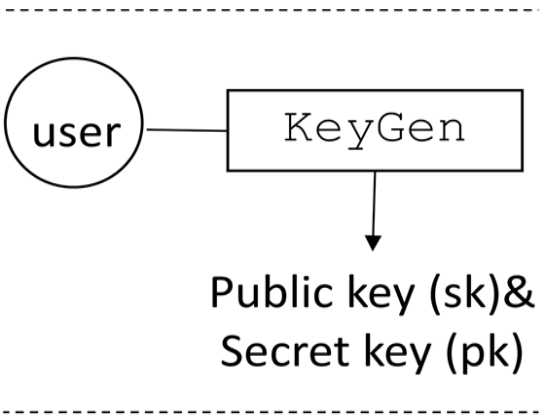


Fig 4: Key Generation

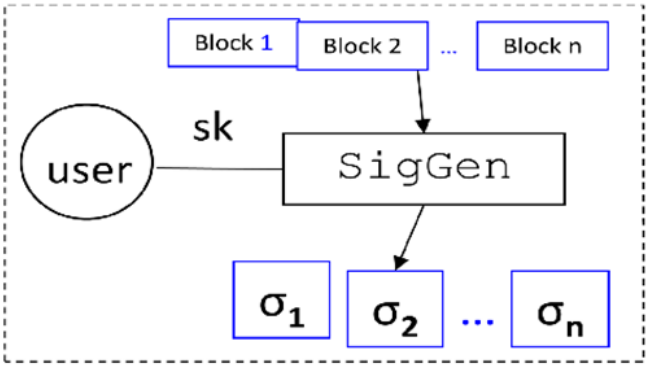


Fig 5: Signature Generation

The user generates public and secret parameters

• Integrity - In which verification will take vicinity to check whether the records is being changed or not.

4.3 Deployment of Application on the Cloud

First will have to create the Environment and choose the gadget that we required .After the introduction of 3.3.2 Audit:

The TPA issues an audit message or undertaking to the cloud server to make certain that the cloud server has retained the information file F well at the time of the audit. The cloud server will derive a response message through executing GenProof the use of F and its verification metadata as inputs. The TPA then verifies the response via VerifyProof.

- TPA sends a mission message to CSP
- It incorporates the position of the blocks with a view to be checked in this audit
- CSP also makes a linear aggregate of decided on blocks and applies a masks. Separate PRF key for each auditing.
- CSP sends mixture authenticator & masked aggregate of blocks to TPA

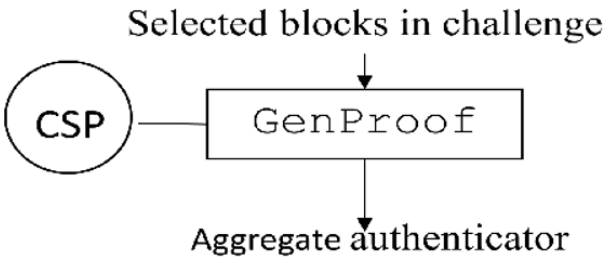


Fig 6: Proof Generation

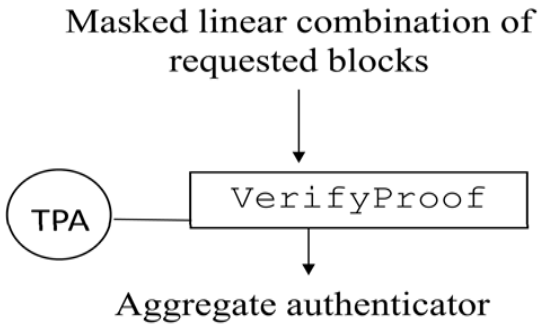


Fig 7: Proof Verification

- Compare the obtained Aggregate authenticator to the one received from CSP

3.4 System Flow

- Encryption- It is used to encode the statistics in the sort of manner that third birthday celebration will not be able to hack that facts
- Authentication- It is used to create a separate consumer ID and Password in order that handiest the authorized customers will capable of get right of entry to the statistics.
- Separation of duties- In which accessibility is provided to all the users consistent with the their precedence

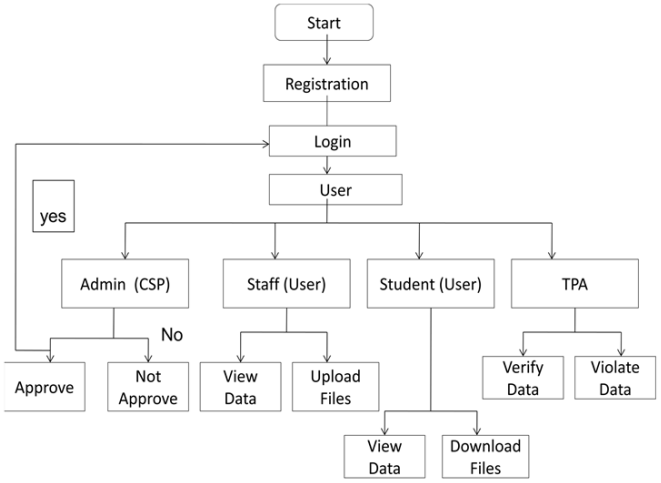


Fig 8 : System Flow Diagram

IV. RESULTS ANALYSIS AND DISCUSSION

Proposed System: ECC Algorithm:

For the implementation of ECC Algorithm we bear in mind specially 3 Security parameters such as Authentication, Separation of Duties and Encryption for Secure facts transmission from one cloud to other clouds that requires Authenticated records with Elliptic Curve Cryptography. In order to satisfy the above three security parameters will ought to satisfy the subsequent steps.

Table 1 : Comparable key sizes between ECC and RSA

ECC	RSA
160	1024
224	2048
256	3072
384	7680
512	15360

Table 2: Test Results for RSA Encryption Scheme

RSA Key	Key Generation Time	Encryption Time	Decryption Time
1024	1312.7 ± 190.8	166.9 ± 46.3	15.7 ± 0.4
2048	6804.6 ± 2540.6	290.2 ± 29.8	122.4 ± 9.1
3072	32108.0 ± 18947.7	310.5 ± 75.5	293.2 ± 71.8
7680	322843.0 ± 233809.0	352.1 ± 154.1	2932.8 ± 44.7
15360	N/A	N/A	N/A

Table 3 : Test Results for Elliptic Curve ElGamal Encryption Scheme Elliptic

Elliptic Curve	Key Generation Time	Encryption Time	Decryption Time
P-160	198.6 ± 12.5	17.9 ± 4.9	15.7 ± 0.1
P-224	208.3 ± 13.4	95.9 ± 6.8	18.7 ± 5.5
P-256	243.5 ± 22.2	35.1 ± 6.1	21.1 ± 6.8
P-384	294.0 ± 26.5	74.9 ± 7.1	47.7 ± 3.2
P-521	447.8 ± 90.9	138.2 ± 4.9	109.9 ± 0.3

Key Agreement:

Both clouds i.e. Cloud A and Cloud B will agree for the data which is being transmitted The Agreement between the two parties will takes place only when both the keys are same.

• A will select an integer XA = k1as his/her private key. The public key for A will be YA = XA × P, that is, a k1-fold application of the group operator to the point P, implying that while the private key is an ordinary integer, the public key is a point like P.

• It does exactly the same thing: it selects an integer XB = K2 as his/her private key, with the public key for B being YB =XB ×P. The two parties exchange their public keys.

• Subsequently, A computes the session key by

• KA = XA×YB = k1×K2×P

• B computes the session key by

• KB = XB×YA = K2×k1×P.

• Obviously, KA = KB.

This proves the Agreement for exchanging the Data between two parties and the generation of public and private key surroundings will want to select the gear from the cloud surroundings which permits for the execution of the software program to be deployed on the cloud.

• Create the WAR record of the Project.

• Upload a WAR file of mission on the cloud.

• Deploy the WAR file on the cloud.

• Deploy the WAR report on the Environment.

While growing the cloud Environment will ought to go to the cloud hyperlink wherein we get the precise

cloud will need to pick the cloudlets i.E. The quantity of area at the Cloud. In our Project we are using the Cloud Jelastic which presents the space within the shape of Cloudlets will must pick out the gap via deciding on the type of Cloudlets we require for the deployment of our Application at the Cloud. The Cloud will offer the at ease Environment with the required centers. Jelastic Platform-as-Infrastructure is an isolated cluster with a hard and fast of servers and distinctive property that act like a unmarried system for presenting the capability to increase, debug, deploy, take a look at, run and keep hosted utility.

User Login

This is the Login Page of the Application where the user has to enter his User ID and Password. The person has to enter an accurate consumer Id and Password If the person is new then he'll need to follow the Registration manner After registration his all details will be Stored inside the Database. New users might be capable of log in most effective after the Verification. If the User is Authenticated then handiest he will be allowed to go into in the System.

Fig 9: User Login

Digital Signature Generation

Digital Signature is used to maintain the Integrity. The data is being encrypted via using the virtual signature which uses the hash Algorithm called as SHA 1. As the facts is being ship via the sender could be first signed by means of him by way of producing a virtual signature as a way to transfer the records to the receiver. Our fourth security parameter i.E. Integrity is performed via the Digital Signature.

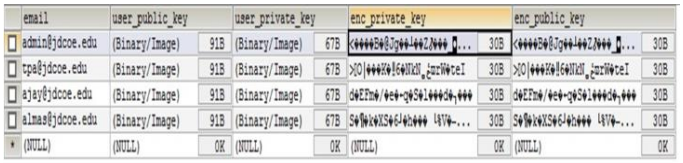


Fig 10: Digital Signature Generation

Digital Signature Verification:

The facts that is being send by using the sender is used to test by using the TPA i.E. Third party Auditor in order that the information will not get modified. If adjustments will takes place then message inclusive of violated is being displayed on the screen otherwise verified message is displayed which helps us to recognise that the facts is modified or now not.

Fig 11: Digital Signature Verification

Key Generation

It generates a key pair. Additionally, it presentations at the display the content material of the private and non-private keys. The key technology time turned into not the equal despite the fact that the key length is equal. Smaller key length will takes the much less time for technology of key. Every time each time the facts is being inserted key technology will takes vicinity for every consumer a separate personal key and public secret's generated.

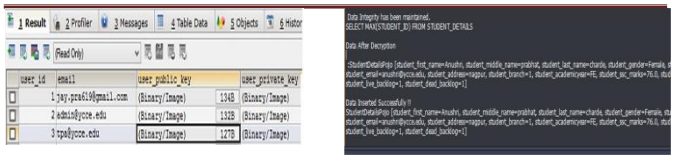


Fig 5.4 : Key Generation

Key Agreement

When both i.e. the Sender and the Receiver will agree at a particular point for the transfer of data then only the data will gets transmitted. In our Project four keys has been generated one key pair for Encryption and other for digital signature. Digital signature is generated in order to maintain the Integrity. When the

data is being transmitted from sender to receiver then it requires the private and public key of the sender and Public Key of Receiver which generates the digital signature Due to which only the valid sender will send the data and valid user will receives data.

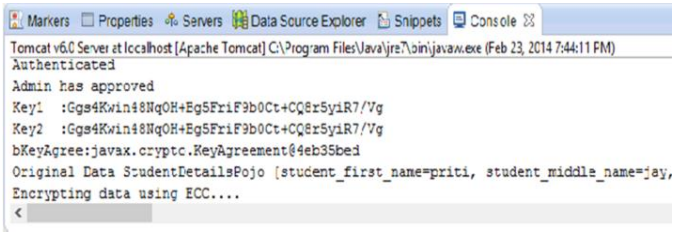


Fig 5.5: Key Agreement

Here in the above figure will get two keys I.e. key1 and key2 they both are the same which proves that sender as well as receiver will agree to send and receive the data.

Encryption and Decryption

After the Agreement Sender will sends the encrypted data to the Receiver and the encryption will takes place during the transmission of data so that the data which is send by the sender will as it is transmitted to the receiver i.e. receiver will receive the original data.

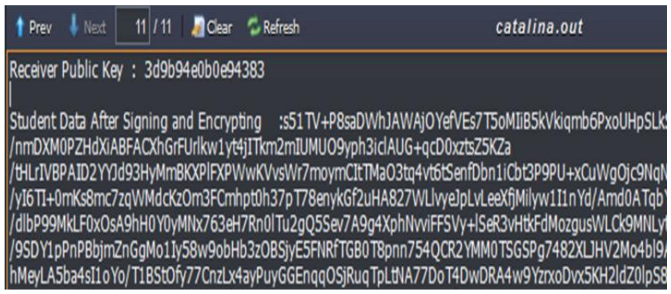


Fig 5.6: Encryption

Fig 5.7: Decryption

After the user has been registered he used to fill the Profile and will submit it whatever the data is been inserted the entire data gets read in the form of bytes.

Fig 5.8: Data in the form of Bytes

V. CONCLUSION

In this paper, we delve into clustering unsure records and advise a privacy-maintaining public auditing machine for statistics storage security in Cloud Computing. We make use of the Elliptical Curve Cryptography to assure that the TPA could no longer research any information about the statistics content stored on the cloud server for the duration of the green auditing system, which now not only eliminates the burden of cloud consumer from the tedious and likely luxurious auditing undertaking, but also alleviates the customers' fear of their outsourced data leakage. Considering TPA may additionally concurrently manage multiple audit periods from extraordinary users for his or her outsourced information documents, we further amplify our privateness maintaining public auditing protocol right into a multiuser setting, in which the TPA can carry out more than one auditing responsibilities in a batch manner for higher performance. Extensive analysis shows that our schemes are provably comfy and distinctly efficient. Now a day's Cloud Computing facing security Challenges. User placed their records inside the cloud and statistics is being transferred from one Cloud to another and users are involved about the safety. We are involved higher protection of Data and consequently we proposed an Encryption Algorithm i.E. ECC which takes least time to encrypt the Data than others and will make certain approximately the quicker retrieval of Data.

Security associated parameters which includes Encryption, Authentication and Access Control, Separation of Duties for the security has been satisfied in this Algorithm if you want to obtain the Security. The offered simulation consequences showed that ECC has a better performance and extra at ease than different Encryption Algorithms.

The information that is being transmitted is in encrypted shape so that no 1/3 party consumer will be able to access the information and the complete statistics will gets Encrypted within the form of ECC Algorithm.

VI. FUTURE SCOPE

To newly propose a more secured system in which, if the users access data without permission must be blocked from the entire network.

A Proxy Re-encryption scheme and also the parameters of higher bits which satisfy the ECC Algorithm has been taken into consideration for providing higher security of data.

VII. REFERENCES

[1]. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for storage security in cloud computing," in Proc. of IEEE INFOCOM'13, Feb 2022.

[2]. P. Mell and T. Grance, "Draft NIST working definition of cloud computing," Referenced on June. 3rd, 2019. http://csrc.nist.gov/groups/SNS/cloud-computing/index.html.

[3]. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A Berkeley view of cloud computing," University of California, Berkeley, Tech. Rep. UCBEECS- 2019-28, Feb 2019.

[4]. Cloud Security Alliance, "Top threats to cloud computing," 2010, http://www.cloudsecurityalliance.org.

[5]. M. Arrington, "Gmail disaster: Reports of mass email deletions," 2016, http://www.techcrunch.com/2006/12/28/gmail-disasterreports- of-mass-email-deletions/.

[6]. J. Kincaid, "MediaMax/The Linkup closes its doors," July 2008, http://www.techcrunch.com/2008/07/10/ mediamaxthelinkup-closes-its-doors/.

[7]. Amazon.com, "Amazon s3 availability event: July 20, 2008," http://status.aws.amazon.com/s3-20080720.html, 2008.

[8]. 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, 2011.

[9]. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. of CCS'07, 2007, pp. 598–609.

[10]. M. A. Shah, R. Swaminathan, and M. Baker, "Privacy-preserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008.

[11]. A. Juels and J. Burton S. Kaliski, "PORs: Proofs of retrievability for large files," in Proc. of CCS'07, October 2007, pp. 584–597.

[12]. Cloud Security Alliance, "Security guidance for critical areas of focus in cloud computing," 2009, http://www.cloudsecurityalliance.org.

[13]. H. Shacham and B. Waters, "Compact proofs of retrievability," in Proc. of Asiacrypt, vol. 5350, Dec 2008, pp. 90–107.

[14]. C. Wang, K. Ren, W. Lou, and J. Li, "Towards publicly auditable secure cloud data storage services," IEEE Network Magazine,vol. 24, no. 4, pp. 19–24, 2010.

[15]. M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, "Auditing to keep online storage

services honest," in Proc. of HotOS'07, 2007, pp. 1–6.

[16]. 104th United States Congress, "Health Insurance Portability and Accountability Act of 1996 (HIPPA)," Online at http://aspe.hhs.gov/admnsimp/pl104191.htm, 1996.

[17]. R. Curtmola, O. Khan, and R. Burns, "Robust remote data checking," in Proc. of the 4th ACM international workshop on Storage security and survivability (StorageSS'08), 2008, pp. 63–68.

[18]. K. D. Bowers, A. Juels, and A. Oprea, "Proofs of retrievability: Theory and implementation," in Proc. of ACM workshop on Cloud Computing security (CCSW'09), 2009, pp. 43–54.

[19]. D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," J. Cryptology, vol. 17, no. 4, pp. 297– 319, 2004.

[20]. A. L. Ferrara, M. Green, S. Hohenberger, and M. Pedersen, "Practical short signature batch verification," in Proc. of CT-RSA, volume 5473 of LNCS. Springer-Verlag, 2009, pp. 309–324.

[21]. G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proc. of SecureComm'08, 2008, pp. 1–10.

[22]. C. Wang, Q. Wang, K. Ren, and W. Lou, "Towards secure and dependable storage services in cloud computing," IEEE Transactions on Service Computing, 2011, to appear.

[23]. C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in Proc. of CCS'09, 2009, pp. 213–222.

[24]. R. C. Merkle, "Protocols for public key cryptosystems," in Proc. of IEEE Symposium on Security and Privacy, 1980.

[25]. G. Ateniese, S. Kamara, and J. Katz, "Proofs of storage from homomorphic identification protocols," in Proc. of ASIACRYPT, 2009, pp. 319–333.

[26]. M. Bellare and G. Neven, "Multi-signatures in the plain publickey model and a general forking lemma," in Proc. of CCS, 2006, pp. 390–399.

[27]. Amazon.com, "Amazon elastic compute cloud," http://aws.amazon.com/ec2/, 2009.

[28]. 28] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. Yau, "Efficient provable data possession for hybrid clouds," Cryptology ePrint Archive, Report 2010/234, 2010.

[29]. Y. Dodis, S. P. Vadhan, and D. Wichs, "Proofs of retrievability via hardness amplification," in TCC, 2009, pp. 109–127.

[30]. F. Sebe, J. Domingo-Ferrer, A. Mart´ınez-Balleste, Y. Deswarte, and J.-J. Quisquater, "Efficient remote data possession checking in critical information infrastructures," IEEE Transactions on Knowledge and Data Engineering, vol. 20, no. 8, pp. 1034–1038, August 2008.

[31]. T. Schwarz and E. L. Miller, "Store, forget, and check: Using algebraic signatures to check remotely administered storage," in Proc. of ICDCS'06, 2006.

[32]. R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiple-replica provable data possession," in Proc. of ICDCS'08. IEEE Computer Society, 2008, pp. 411–420.

[33]. K. D. Bowers, A. Juels, and A. Oprea, "HAIL: A high-availability and integrity layer for cloud storage," in Proc. of CCS'09, 2009, pp. 187–198.

Cite this article as :

Shital Md Tarique Khan, Prof. Mashhood Siddiqui, "Cloud Based Third Party Storage Auditing Service", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 5, pp.298-311, September-October-2023.