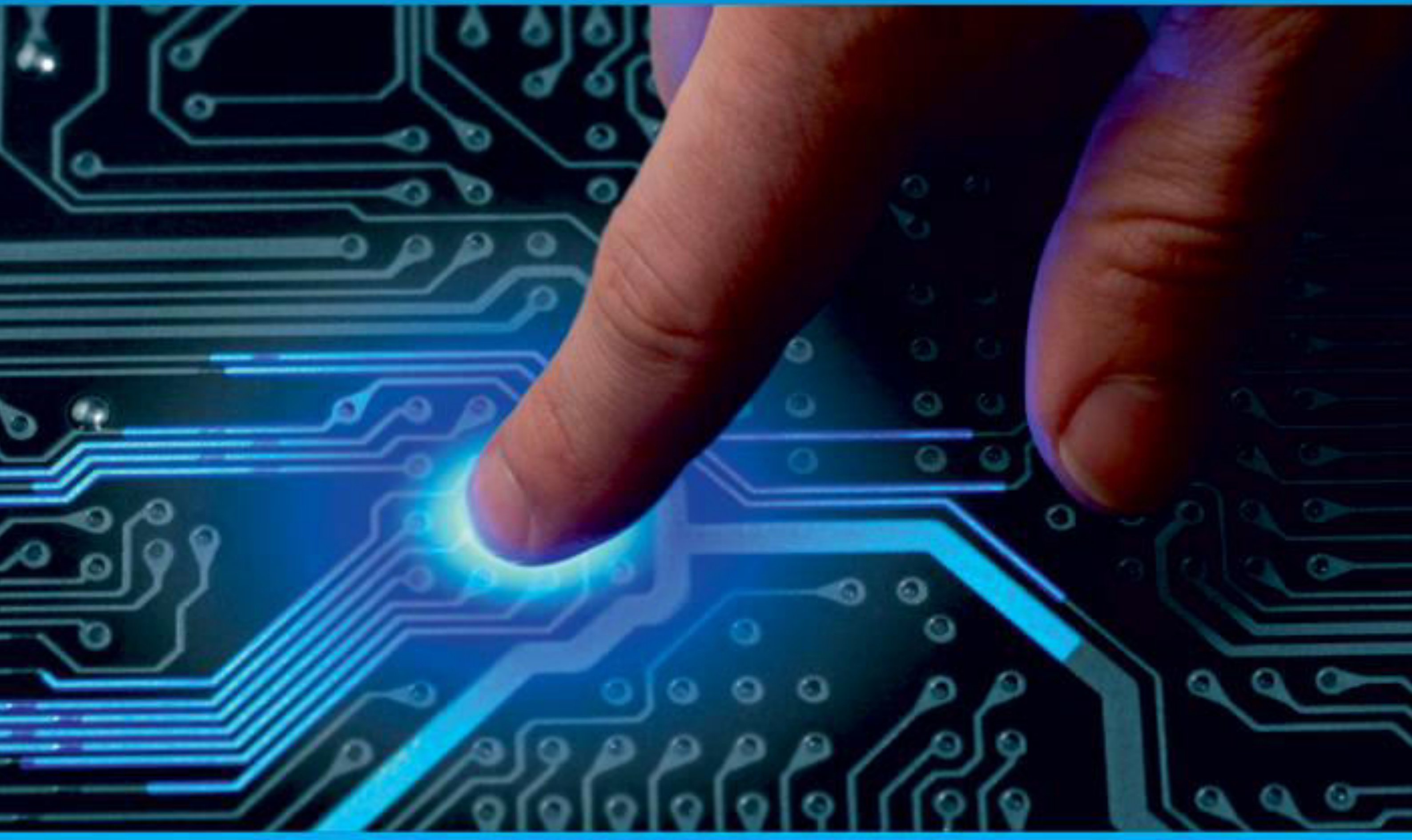
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 8, August 2022

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.165

Privacy Preserving Public Auditing For Secure Clode

Nafeesa banu, Usha C

Student, Department of MCA, University B.D.T.C.E, Davanagere, India

Assistant Professor, Department of Master of Computer Applications, University B.D.T.C.E, Davanagere, India

ABSTRACT: With the large-scale application of cloud storage, how to ensure cloud data integrity has become an important issue. Although many methods have been proposed, they still have their limitations. This paper improves some defects of the previous methods and proposes an efficient cloud data integrity verification scheme based on blockchain. In this paper, we proposed a lattice signature algorithm to resist quantum computing and introduced cuckoo filter to simplify the computational overhead of the user verification phase. Finally, the decentralized blockchain network is introduced to replace traditional centralized audit to publicize and authenticate the verification results, which improves the transparency and the security of this scheme. Security analysis shows that our scheme can resist malicious attacks and experimental results show that our scheme has high efficiency, especially in the user verification phase.

I. INTRODUCTION

With lots of applications deployed in the cloud, user data are also collected centrally and handed over to the cloud. Cloud computing provides users with shared computing resources and storage resources and has multiple deployment models like private cloud, community cloud, public cloud, and hybrid cloud [1]. For users, storing data in the cloud can bring many benefits, such as reducing hardware investment costs, reducing the local storage burden, and supporting remote access. However, while cloud storage brings convenience, it also brings corresponding challenges. Highly centralized data and complex computing environments make user data subject to multiple threats [2]. Compared to traditional data center, the cloud has more complex systems. The numerous components make the cloud more likely to be attacked. As the complexity of the systems increases, so do the vulnerabilities of the systems. Secondly, multitenant share cloud computing resources, making data more vulnerable to be damaged. In the cloud computing environment, the customized resources between tenants are usually isolated by adopting a logical method. A malicious attacker may pretend to be a tenant to launch an internal attack, violating other users' data. Finally, cloud service providers may deliberately hide that user data are corrupted or store data that users rarely access offline. Considering the large-scale outsourcing data and limited computing power, verifying outsourcing data integrity has become a vital issue in cloud storage.

The root problem of cloud data security lies in the trust between the cloud service provider (CSP) and the user. Failure of cloud devices, external attacks, or even the snooping of user data by the CSPs may result in leakage, loss, and damage of user data. On the other hand, even if user data is destroyed, users may not achieve effective accountability, and the CSP will evade responsibility and not recognize it. Therefore, the essence of the problem lies in the lack of trust between the two sides. Once problems occur, it is difficult for the challenged party to provide the basis agreed by both sides.

This paper proposes a protocol for cloud data integrity verification based on lattice signature. Under the small integer solution (SIS) assumption, the algorithm can resist quantum attacks and malicious attacks under the random oracle model and protect user data privacy. The user's computational complexity in the verification phase is greatly simplified by introducing the cuckoo filter, and the algorithm's efficiency is further improved.

II. LITERATURE REVIEW

Computing is a new term for a long-held dream of computing as a utility [35], which has recently emerged as a commercial reality. Cloud Computing is likely to have the same impact on software that foundries have had on the

-Berkeley and M. Armbrust

2. The interesting thing about Cloud Computing is that we've redefined Cloud Computing to include everything that we already do. . . . I don't understand what we would do differently in the light of Cloud Computing other than change the wording of some of our ads

-Larry Ellison, quoted in the Wall Street Journal, September 26, 2008

3. A lot of people are jumping on the [cloud] bandwagon, but I have not heard two people say the same thing about it. There are multiple definitions out there of "the cloud."
-Andy Isherwood, quoted in ZDnet News, December 11, 2008

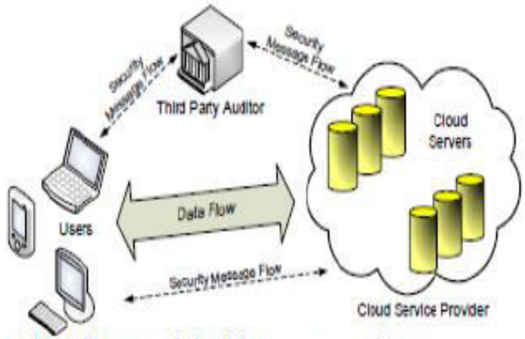
4. MAC Based Solution

It is used to authenticate the data. In this, user upload data blocks and MAC to CS provide its secret key SK to TPA. The TPA will randomly retrieve data blocks & Mac uses secret key to check correctness of stored data on the cloud. Problems with this system are listed below as

- It introduces additional online burden to users due to limited use (i.e. Bounded usage).
- Communication & computation complexity
- TPA requires knowledge of data blocks for verification
- Limitation on data files to be audited as secret keys are fixed
- After usages of all possible secret keys, the user has to download all the data to
Re computed MAC & republish it on CS.
- TPA should maintain & update states for TPA which is very difficult
- It supports only for static data not for dynamic data.

5. HLA Based Solution

It supports efficient public auditing without retrieving data block. It is aggregated and required constant bandwidth. It is possible to compute an aggregate HLA which authenticates a
linear combination of the individual data blocks



: The architecture of cloud data storage services

6.Privacy Preserving Public Auditing Proposed by Cong Wang

Public auditing allows TPA along with user to check the integrity of the outsourced data stored on a cloud & Privacy Preserving allows TPA to do auditing without requesting for local copy of the data. Through this scheme [1], TPA can audit the data and cloud data privacy is maintained. It contains4 algorithms as

1) **Key-gen***:* It is a key generation algorithm used by the user to setup the scheme.

2) **Sing-en***:* It is used by the user to generate verification metadata which may include digital signature.

3) **GenProof***:* It is used by CS to generate a proof of data storage correctness.

4) **Verifyproof***:* Used by TPA to audit the proofs

III. SYSTEM'S ARCHITECTURE

The Scope of this paper is to implement "Preserving Integrity of Data and Public Auditing for Data Storage Security in Cloud Computing" to Provide Efficient Storage of public Data in a cloud.

IV. METHODOLOGY

CLOUD Computing has been envisioned as thenext-generation information technology (IT) architecturefor enterprises, due to its long list of unprecedentedadvantages in the IT history: on-demandself-service, ubiquitous network access, location independentresource pooling, rapid resource elasticity,usage-based pricing and transference of risk.a disruptive technology with profound implications,Cloud Computing is transforming the very nature ofhow businesses use information technology. One fundamentalaspect of this paradigm shifting is that details being centralized or outsourced to the Cloud.

Fromusers' perspective, including both individuals and ITenterprises, storing data remotely to the cloud in aflexible on-demand manner brings appealing benefits: relief of the burden for storage management, universaldata access with independent geographical locations, and avoidance of capital expenditure on hardware,software, and personnel maintenances, etc.

While Cloud Computing makes these advantages more appealing than ever, it also brings new and challengingsecurity threats towards users' outsourced-data. Since cloud service providers (CSP) are separate administrative entities, data outsourcing is actually relinquishing user's ultimate control over the fate of their data. As a result, the correctness of the datain the cloud is being put at risk due to the following reasons.

First of all, although the infrastructuresunder the cloud are much more powerful and reliablethan personal computing devices, they are stillfacing the broad range of both internal and external Threats for data integrity. Examples of outages andsecurity breaches of noteworthy cloud services appear from time to time.

Secondly, there do existvarious motivations for CSP to behave unfaithfullytowards the cloud users regarding the status of theirout-sourced data. For examples, CSP might reclaimstorage for monetary reasons by discarding data that has not been or is rarely accessed, or even hide dataloss incidents so as to maintain a reputation.

-In short, although outsourcing data to the cloud is economically attractive for long-term large-scale data storage, it does not immediately offer any guaranteeon data integrity and availability. This problem, Ifnot properly addressed, may impede the successfuldeployment of the cloud architecture.

-As users no longer physically possess the storage oftheir data, traditional cryptographic primitives for thepurpose of data security protection cannot be directlyadopted. In particular, simply downloading allthe data for its integrity verification is not a practicalsolution due to the expensiveness in I/O and transmissioncost across the network. Besides, it is ofteninsufficient to detect the data corruption only when accessing the data, as it does not give users correctness assurance for those uncased data and might be toolate to recover the data loss or damage. Considering the large size of the outsourced data and the user'sconstrained resource capability, the tasks of auditingthe data correctness in a cloud environment can beformidable and expensive for the cloud users. Moreover, the overhead of using cloud storageshould be minimized as much as possible, such that user does not need to perform too many operations to use the data (in additional to retrieving the data)

.

Existing System

The cloud data storage service contains 3 different entitiesas cloud user, Third party auditor &cloud server / cloud Service provider. Cloud user is a person who stores large amount of data or files on a cloud server. Cloud server is aplace where we are storing cloud data and that data will bemanaged by the cloud service provider. Third party auditors will do the auditing on users request for storage correctnessand integrity of data.

Security Issues

The security is a major issue in cloud computing. It is a subdomain of computer security, network security or else datasecurity. The cloud computing security refers to a broad set ofpolicies, technology & controls deployed to protect data,application & the associated infrastructure of cloud computing.Some security and privacy issues that need to be consideredare as follows:

i) Authentication*:* Only authorized user can access data inthe cloud

ii) Correctness of data*:* This is the way through whichuser will get the confirmation that the data stored in thecloud is secure

iii) Availability*:* The cloud data should be easily availableand accessible without any burden. The user shouldaccess the cloud data as if he is accessing local data

iv) No storage Overhead and easy maintenance: Userdoesn't have to worry about the storage requirement &maintenance of the data on a cloud

v) No data Leakage: The user data stored on a cloud canaccessed by only authorize the user or owner. So all thecontents are accessible by only authorize the user.

vi) No Data Loss: Provider may hide data loss on a cloudfor the user to maintain their reputation.

Solution Statement

Recently, the notion of public auditability has beenproposed in the context of ensuring remotely storeddata integrity under different system and securitymodels. Public auditability allowsan external party, in addition to the user himself,to verify the

correctness of remotely stored data.However, most of these schemes do notconsider the privacy protection of users' data againstexternal auditors. Indeed, they may potentially revealuser data information to the auditors. This severe drawbackgreatly affects the security of these protocols in CloudComputing. From the perspective of protecting data privacy, the users, who own the data and rely onTPA just for the storage security of their data, do notwant this auditing process introducing new vulnerabilitiesof unauthorized information leakage towards their data security. Moreover, there are legalregulations, such as the US Health Insurance Portabilityand Accountability Act, furtherdemanding the outsourced data not to be leaked toexternal parties. Exploiting data encryption before outsourcing is one way to mitigate this privacy concern, but it is only complementary to the privacypreservingpublic auditing scheme to be proposedin this paper. Without a properly designed auditingprotocol, encryption itself cannot prevent data from"flowing away" towards external parties during theauditing process. Thus, it does not completely solvethe problem of protecting data privacy but just reducesit to the key management. Unauthorized dataleakage still remains a problem due to the potentialexposure of decryption keys.
Besides, with the prevalence of Cloud Computing, a foreseeable increase of auditing tasks from differentusers may be delegated to TPA. As the individualauditing of these growing tasks can be tedious andcumbersome, a natural demand is then how to enablethe TPA to efficiently perform multiple auditing tasksin a batch manner, i.e., simultaneously.To address these problems, our work utilizes thetechnique of public key based homomorphism linear authenticator whichenables TPA to perform the auditing without demanding the local copy of data and thus drastically reducesthe communication and computation overheadas compared to the straightforward data auditingapproaches. By integrating the HLA with randommasking, our protocol guarantees that the TPA couldnot learn any knowledge about the data contentstored in the cloud server during the efficient auditingprocess. The aggregation and algebraic properties of the authenticator further benefit our design for thebatch auditing.

Proposed System

The proposed system specifies that user can access the dataon a cloud as if the local one without worrying about theintegrity of the data. Hence, TPA is used to check the integrity of data. It supports privacy preserving public auditing. Itchecks the integrity of the data, storage correctness. It alsosupports data dynamics & batch auditing. The major benefitsof storing data on a cloud is the relief of burden for storagemanagement, universal data access with location independent& avoidance of capital expenditure on hardware, software &personal maintenance.
In cloud, data is stored in a centralized form and managing his data and providing security is a difficult task. TPA canread the contents of data owner hence can modify. Thereliability is increased as data is handled by TPA but dataintegrity is not achieved. It uses encryption technique toencrypt the contents of the file.TPA checks the integrity of the data stored on a cloud but ifthe TPA itself leaks the user's data. Hence the new conceptcomes as auditing with zero knowledge privacy where TPAwill audit the users' data without seeing the contents. It usespublic key based linear authentication (HLA) which allows TPA to perform auditing withoutrequesting for user data. It reduces communication &computation overhead. In this, HLA with random maskingprotocol is used which does not allow TPA to learn datacontent.

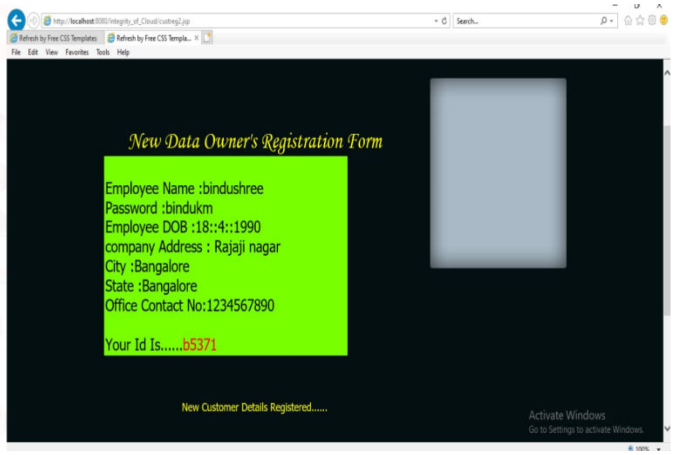
V. RESULT AND DISCUSSION

This paper evaluates the correctness and feasibility of the proposed method through experiments. Experimental results show that the method is effective.

-With lots of applications deployed in the cloud, user data are also collected centrally and handed over to the cloud. Cloud computing provides users with shared computing resources and storage resources and has multiple deployment models like private cloud, community cloud, public cloud, and hybrid cloud [1]. For users, storing data in the cloud can bring many benefits, such as reducing hardware investment costs, reducing the local storage burden, and supporting remote access. However, while cloud storage brings convenience, it also brings corresponding challenges. Highly centralized data and complex computing environments make user data subject to multiple threats [2]. Compared to traditional data , the cloud has more complex systems. The numerous components make the cloud more likely to be attacked. As the complexity of the systems increases, so do the vulnerabilities of the systems. Secondly, multitenantshare cloud computing resources, making data more vulnerable to be damaged. In the cloud computing environment, the customized resources between tenants are usually isolated by adopting a logical method. A malicious attacker may pretend to be a tenant to launch an internal attack, violating other users' data. Finally, cloud service providers may deliberately hide that user data are corrupted or store data that users rarely access offline. Considering the large-scale outsourcing data and limited computing power, verifying outsourcing data integrity has become a vital issue in cloud storage.

The root problem of cloud data security lies in the trust between the cloud service provider (CSP) and the user. Failure of cloud devices, external attacks, or even the snooping of user data by the CSPs may result in leakage, loss, and damage of user data. On the other hand, even if user data is destroyed, users may not achieve effective accountability, and the CSP will evade responsibility and not recognize it. Therefore, the essence of the problem lies in the lack of trust between the two sides. Once problems occur, it is difficult for the challenged party to provide the basis agreed by both sides.

Original Dataset:


http://localhost:8080/Integrity_of_Cloud/custreg2.jsp
Search...
Refresh by Free CSS Templates
Refresh by Free CSS Templa...
File Edit View Favorites Tools Help

New Data Owner's Registration Form

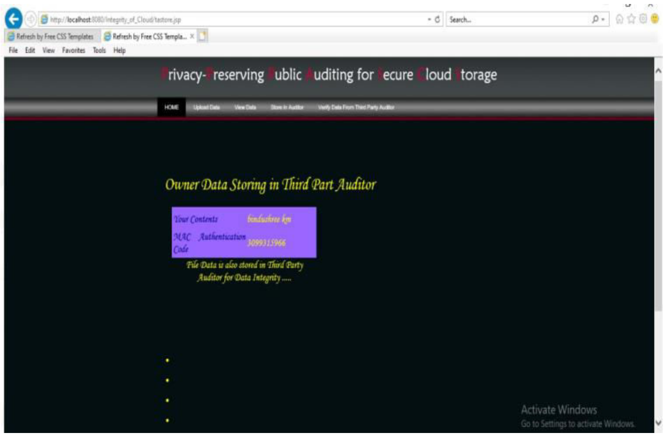
Employee Name :bindushree
Password :bindukm
Employee DOB :18::4::1990
company Address : Rajaji nagar
City :Bangalore
State :Bangalore
Office Contact No:1234567890

Your Id Is......b5371

New Customer Details Registered......

Activate Windows
Go to Settings to activate Windows.
100%

User Registration and generate ID for the user


http://localhost:8080/Integrity_of_Cloud/tastore.jsp
Search...
Refresh by Free CSS Templates
Refresh by Free CSS Templa...
File Edit View Favorites Tools Help
Privacy-Preserving Public Auditing for Secure Cloud Storage
HOME
Upload Data
View Data
Store in Auditor
Verify Data From Third Party Auditor

Owner Data Storing in Third Part Auditor

Your Contents	bindushree km
MAC Authentication Code	3099315966

File Data is also stored in Third Party Auditor for Data Integrity .....

Activate Windows
Go to Settings to activate Windows.

Data being uploaded on TPA

VI. CONCLUSION

The goal of this project is to improve security for the data integration problem, by this technique we can identify any data modification on uploaded data, if any one modified uploaded data then it is identified and ignored. The proposed framework determines that client can get to the information on a cloud as though the neighborhood one without agonizing over the trustworthiness of the information. Subsequently, TPA is utilized to check the trustworthiness of information. It upholds security protecting public evaluating. It checks the uprightness of the information, stockpiling accuracy.

REFERENCES

[1] A. Fox, R. Griffith, A.Joseph, R. Katz, A. Kaminski, G. Lee, D. Patterson, A.Rabin, and I.Stoica, "Above the clouds: A Berkeley view of cloud computing," Dept. Electrical Eng. And Computer Sciences, University of California, Berkeley ,Rep. UCB/EECS, vol. 28,p. 13, 2009.

[2] G. Ateniese, R. Burns, R. Curtmola. J. Herring, L. Kissner. Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proceedings of the 14TH ACM Conference on Computer and Communication Security, ser. CCS '07. New York, NY, USA: ACM, 2007,pp. 598-609.

[3] A. Juels and B. S. Kaliskijr. "pors:Proofs of retrievability for large files, "in Proceeding of the 14th ACM conference on Computer and communication security . ACM. 2007,pp. 584-597.

[4] R. Curtmola. O. Khan. R. Burns "Mr-pdp: Multiplereplica provable datapossession." In Distributed Computin System, 2008. ICDCS'08. The 28thInternational Conference on IEEE, 2008, pp. 411-420.

[5] K. D. Bowers. A. Juels. And A. Oprea. "Hail: a high-availability and integrity layer for cloud storage," in Proceedings of the 16th ACM conference on Computer and communications security . ACM. 2009. Pp. 187-198.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details