JOURNAL OF BASIC SCIENCE AND ENGINEERING

AMACBASED BLOCK CHAIN FOR EFFICIENT DATA INTEGRITY VERIFICATION SCHEME IN MULTI- CLOUD STORAGE

Dr. A.S.Muthanantha Murugavel

Professor, Department of CSE

Karpagam College of Engineering

Coimbatore Tamilnadu,

murugavel.asm@gmail.com

Jeyanth.K

Department of Computer Science and Engineering

Karpagam College of Engineering

Coimbatore-641032,Tamilnadu, India

jeyanthsoloist@gmail.com

Karan.V

Department of Computer Science and Engineering

Karpagam College of Engineering

Coimbatore-641032, Tamilnadu, India

Mohammed Mahir.S

Department of Computer Science and Engineering

Karpagam College of Engineering

Coimbatore-641032,Tamilnadu, India

Naveen Prasad R

Department of Computer Science and Engineering

Karpagam College of Engineering

Coimbatore-641032, Tamilnadu, India

Abstract— Massive data access and storage are made possible by cloud storage services, which also lowers the cost of managing massive data volumes. Users can use cloud storage's data integrity verification scheme to help verify the accuracy of data that has been outsourced. Whilethird-partyauditors(TPAs)canbehiredtohandle data integrity verification

through public data integrity verification schemes, there are still numerous security andoperationalissueswithcentralizedTPA.Researchers have attempted to use blockchain technology to address the centralization issue with conventional methods in recentyears,buttheseplansignoretheissueofefficiency degradation brought on by the use of blockchain technology. An effective data integrity MAC verification method for multi-cloud storage services is proposed in this work.

I. INTRODUCTION

- Z convenient with the centralized TPA'sparticipation, there are still a lot of security and efficiency issues. For instance, TPA may save money by avoiding multiple verification processes after a successful verification and producing a report without issues if it is aware that the public audit process is carried out on a regular basis. TPA may also work in concert with the CSP to cover up data corruption from users or to only verify data.
- A distributed database system, which blockchain technology currently offers, has the ability to createa decentralized, fair, and trustworthy cloud storage environment.Fewpeopleareabletoalterdataonceit isontheblockchain,whichmakesitdifficulttoforge, trace, or tamper with because the blockchain records every transaction. Based on blockchain technology, researchers have created a few data audit schemes for data integrity verification in recent years. In order to enable trusted storage of TPA audit logs and assist users in keeping an eye on untrusted TPAs, certain studies have turned to blockchain. Based on this, researchersaregoingtouseblockchaininsteadofTPA for trusted auditing.
- To solve the aforementioned problems, this work suggestsa blockchain-based data integrity verification scheme for multicloudstorage.By puttingthedataverificationprocess directly in theblockchain forpublic execution and offering data integrity verificationserviceswithouttheassistanceof any TPA platform, this paper avoids the security problems brought on by untrusted TPA. This is due to the fact that data on the blockchain is both traceable and unchangeable. Additionally, by achieving the integrity verification of multiple CSPs for multiple DOs, the overall verification resolves the low computational efficiencyissues.Whenthe specific CSP with integrity damage is found through local verification, the problem of locating malicious CSPs in distributed cloud storage is solved. List the units that were applied to each quantity.

II. EXISTINGSYSTEM

- Using traditional cryptographic techniques, such as the well-known public key encryption method, is a simplewaytoprotectdataintegrity.Alimitednumber of keys for the data files that will be outsourced can first be kept locally by data owners. The data owner canverifytheintegrityofthefilewhenevershe needs to retrieve it by recalculating the key of the received data file and comparing it to the locally precomputed value.

- The accuracy of other data that has been outsourced is notguaranteedbythistechnique,eventhoughitallows data owners to verify the accuracy of data they have received from the cloud. Stated differently, there is no assurancethatthedataisactuallyintactunlessthe owner downloads all of the data from the cloud..

III. LIMITATIONSOFEXISTINGSYSTEM

- Given the potential size of cloud data, it would be very impracticalfor adataownertoretrieveallofherdata just to make sure it is still accurate.

- This approach will invariably breach ourrecommended guidelines if thedata auditing work is assigned to aTPA, as it will incur significant auditing expensesfor a cloud server (toaccessandtransferalldata)andexposeTPAdataprivacy (to retrieve a local copy of data).Writers and Connections

V.PROPOSEDSYSTEM

1)We use this authenticator technique by using Merkel- based Message Authentication Codes (MACs) to drastically reduce the arbitrarily large communication overhead for public auditability without adding any online burden to the data owner. Here, authenticators are unchangeable metadata created from individual datablocksthatcanbesafelycombinedtoguarantee

to a verifier that, by confirming the aggregated authenticator alone, a linear combination of data blocksiscomputedcorrectly.Beforeoutsourcing,this methodnecessitatesencodingadditionaldatawiththe data.

ADVANTAGESOFPROPOSEDSYSTEM

- Itachievesaconstantcommunicationoverheadforpublic auditability
- Individual data operations on any file block, especially block insertion and deletion, will no longer affect other unchanged blocks.
- Its exceptional flexibility makes it applicable to medium- sized and even small IT systems, as well as large IT companies and Internet companies.

V.DESIGNANDIMPLEMENTATION

- Firstly, the overhead that theauditing process placeson thecloudservermustnotexceeditsadvantages.Boththe I/O cost and the bandwidth cost associated with data access and transfer may be included in this overhead. Additionally,adataownershouldhaveaslittleadditional onlineburdenaspossible.Thedataownershouldideally be able to relax about storage auditing accuracy and simplyenjoythecloudstorageservicefollowingauditing delegation.

ProtectDataPrivacy:

A service level agreement for cloud storage services has always included data privacy protection as a key component. Therefore, the owner's right to data privacy shouldn't be violated by the adoption of a public auditing protocol. Put differently, a TPAought to becapableof effectively auditing cloud data storage without requiring a local copy of the data or even having to understand the content of the data.

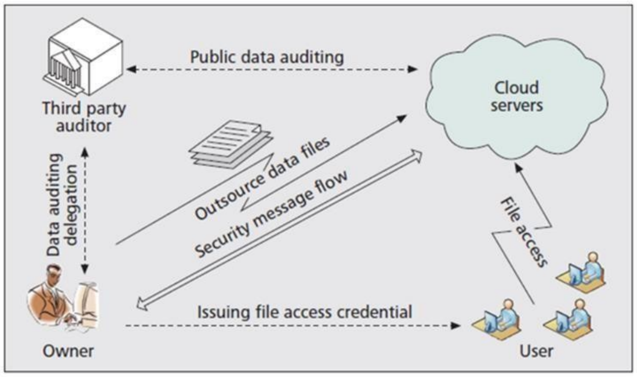
SupportData Dynamics:

Owners must dynamically update their data for a varietyofapplicationpurposes,sincecloudstorageservices are more than just data warehouses. This crucial aspect of cloud computing's data dynamics should be incorporated into the auditing protocol's design.

SupportBatchAuditing:

Large-scale cloud storage services are increasingly common, which raises the bar for auditing effectiveness. Even when a TPA receives numerous auditing tasks from various owners' delegations, it should still be able to complete them quickly and economically. This feature might effectively make it possible for apublic auditing service to grow even in the presence of numerous data owners in a storage cloud.

VIARCHITECTURALDIAGRAM



The interface between the user and the information systemis the input design. and data preparation procedures, which are required to transform transaction data into a format that can be processed. This can be done by having people key dataintothesystemdirectly,orbyhavingthecomputerread data from a written or printed document. Controlling the amount of input needed, reducing errors, preventing delays, eliminating unnecessary steps, and simplifying the process are the main goals of input design. The input is made in a way that maintains privacy while offering security and usability. Input Design took into account the following:

- Whatdatashouldbegivenasinput?
- Howthedatashouldbearrangedorcoded?
- The dialog to guide the operating personnel in providing input.
- Methodsforpreparinginputvalidationsandsteps to follow when error occur.

OBJECTIVES

- Input design is the process of converting a user- oriented description of the input into a computer- based system. This design is crucial for preventing errors in the data input process and guiding managementinobtainingaccurateinformationfrom the computerized system.
- Itisachievedbycreatinguser-friendlyinterfacesfor dataentrytomanagelargevolumesofdata.Thegoal of designing input is to make data entry easier and error-free.Thedataentryscreenisdesignedinsuch awaythatalldatamanipulationscanbeperformed. It also provides record viewing facilities.
- When the data is entered, it will be checked for validity. Data can be entered using screens. Appropriatemessagesareprovidedwhenneededso thattheuserwillnotbeconfusedinstantly.Thus,the objectiveofinputdesignisto createaninputlayout that is easy to follow.

DATABASEDESIGN

Databasesaretypicallybuiltusingapackageknownas a Data Base Management System. Each DBMS has unique characteristics, so general database design techniquesarelimited.E.F.Codd'sworkonrelational databaseshasledtothedevelopmentofoneofthemost practical techniques for analyzing the data needed by the system for the data dictionary. This data analysis techniqueisknownas"Normalization."Threesteps

are involved in the conversion of unnormalized data into normalized data. There is a process to follow at each level.

NORMALIZATION:

Normalization begins with reducing the data to its initial normal form. This is done by eliminating duplicate items and presenting them as distinct records while retaining the important fields from the original record.

The next step in the reduction process to the second normal form is to verify that every item in the first normal form record depends solely on the record's key. A data item is deleted along with its key to createanewrecordifitdependsonanother dataitemrather thantherecord'skey. Thisprocess continuesuntileveryrecordhasdataitemsthatare totally reliant on the key associated with that record.

BUSINESSMODELING:

The information flow among business function is modeled in a way that answers the following questions: what information drives the business process? What information is generated? What generate it? Where does the information go? Who process it?

DATAMODELING:

The information flow defined as a process of the business modeling is refined into a set of dataobjects that are needed to support the business. The characteristics (called attributes) of each object are identifiedandrelationshipsbetweentheseobjectsare defined.

PROCESSMODELING:

The data objects defined in the data-modeling phase are transformed to achieve the information flow necessary to implement a business function. Processing description is created for addition, modifying, deleting, or retrieving a data object.

In Feasibility this stage problem was defined. Criteria for choosing solution were developed, proposed possible solution, estimated costs and benefits of the system and recommended the course of action to be taken.

REQUIREMENTANALYSIS

High-level requirements, such as what the system has to be able todo to solve aproblem, are identified during requirement analysis. To better characterize the features and incorporate them into the proposed system, function requirements and performance requirements for the hardware were expanded upon and made more precise during the initial planning phase.

EXTERNALDESIGN

Creating, organizing, and defining the software product's externally observable characteristics is the externaldesignphaseofanysoftwaredevelopment

process. These features include the functional aspects as well as user displays, report formats, external data sources, and data links.

INTERNA DESIGN ARCHITECTURALAND DETAILED DESIGN

Internal design entailed conceiving, planning, and specifying the internal structure, aswell asprocessing details to record design decisions and explain why certainalternationswerepreferredoverothers.During these stages, test plans are also developed and blueprints for implementation, testing, and maintenance tasks are provided. The architectural structure specification is the end result of internal design.

Thearchitecturalstructurespecification,algorithmic details, data structure details,and testplan arethe end products of internal design work. The conceptual perspective is refined in architectural design.

DETAILEDDESIGN

Detailed design involved specifying the algorithmic details concerned with data representation, interconnections among data structures and packaging of the software product. This phase emphasizes more on semantic issues and less synthetic details.

CODING

Thisphaseinvolvesactualprogramming,i.e,transacting detailed design into source code using appropriate programming language.

DEBUGGING

Thisstagewasrelated with removingerrorsfrom programsandmakingthemcompletelyerrorfree.

MAINTENANCE

During this stage the systems are loaded and put into use. Theyalsogetmodifiedaccordinglytotherequirementsof the user. These modifications included making enhancements to system and removing problems.

CONCLUSIONS

One vision of enterprise IT architecture for the future is cloud computing. Unlike conventional enterprise IT solutions, which maintain appropriate physical, logical,and personnel controls over the IT services, cloud computing relocates the databases and applicationsoftware to servers located in sizable online data centers, where the security of the data and services iscompromised.

Thisspecialqualitycreatesanumberofpreviously unidentified legal and security concerns, including regulatorycomplianceandauditing,aswellasnew security challenges in areas like software and data security, recovery, and privacy.

Weconcentrateonclouddatastoragesecurityinthis work. In order to effectively describe, develop, and evaluatesecuredatastorageproblems,wefirstpresent network architecture..

SCOPEFORFURTHERENHANCEMENT

In the preceding sections, we have outlined recommended requirements for public auditing services and the currentstate of the art that meets these requirements. However, thisis still not sufficient for a publicly auditable secure clouddata storage system, and there are further challenging issues that need to be addressed and resolved. Security in cloud computing,anareafraughtwithchallengesandofparamount importance, is still in its infancy. However, it is expected to attract significant research efforts for many years to come. The final stage of the analysis, the to of third form, form involves examining record that one in the in second normal form determine see whether any items are mutually dependent. If there are any items that are removed to a separate record, one of the items is left behind in the original record and used as the key in the newly created record.

REFERENCES

[1] M.Azhagiri,R.Amrita,R.Aparna,andB.Jashmitha, ``Secured electronic health record management system,'' in Proc. 3rd Int. Conf. Commun.Electron.Syst. (ICCES), Oct. 2018, pp. 915_919.

[2]N.Dong,H.Jonker,andJ.Pang,``Challengesinehealth: From enabling to enforcing privacy,'' in Proc. Int. Symp. Found. Health Informat. Eng. Syst. Cham, Switzerland: Springer, 2011, pp. 195_206.

[3] X.Yi,Y.Miao,E.Bertino,andJ.Willemson, ``Multipartyprivacyprotectionforelectronichealthrecords,'' in Proc.IEEE Global Commun. Conf.(GLOBECOM), Dec. 2013, pp. 2730_2735.

[4] C. S. Kruse, M. Mileski, A. G. Vijaykumar, S. V. Viswanathan, U. Suskandla, and Y. Chidambaram, ``Impact of electronic health records on long-term care facilities: Systematic review,'' JMIR Med. Informat., vol.5,no.3,p.e35,Sep.2017.

[5] Y. Al-Issa, M. A. Ottom, and A. Tamrawi, ``EHealth cloudsecuritychallenges:Asurvey,''J.HealthcareEng.,vol. 2019, pp. 1_15, Sep. 2019.

[6] H.K.Thakkar,C.K.Dehury,andP.K.Sahoo, ``MUVINE:Multi-stagevirtualnetworkembeddingincloud datacentersusingreinforcementlearning-basedpredictions,'' IEEE J. Sel. Areas Commun., vol. 38, no.6, pp. 1058_1074, Jun. 2020.

[7]H.K.Thakkar,P.K.Sahoo,andB.Veeravalli,``RENDA: Resource and network aware data placement algorithm for periodic workloads in cloud,'' IEEE Trans. Parallel Distrib. Syst., vol. 32, no. 12, pp. 2906_2920,
Dec.2021.

[8]J.Zaki,S.M.R.Islam,N.S.Alghamdi,M.Abdullah-Al- Wadud,andK.-S.Kwak,``Introducingcloud-assistedmicro- service-based software development framework for healthcare systems,'' IEEE Access, vol. 10,
pp.33332_33348,2022.

[9] S. Khatri,F.A.Alzahrani,M.T.J.Ansari,A.Agrawal,
R. Kumar, and R. A. Khan, ``A systematic analysis on blockchain integration with healthcare domain: Scope and challenges,'' IEEE Access, vol. 9,pp. 84666_84687, 2021.

[10]S. U. Amin and M. S. Hossain, ``Edge intelligence and Internet of Things in healthcare: A survey,'' IEEE Access, vol. 9, pp. 45_59, 2021.

[11]S. Ali, S.Khusro, andA. Rauf,``A cryptography-based approach to web mashup security,'' in Proc. Int. Conf. Comput. Netw. Inf. Technol., Jul. 2011, pp. 53_57.

[12] E. AbuKhousa, N. Mohamed, and J. Al-Jaroodi, ``e-Healthcloud:Opportunitiesandchallenges,''FutureInternet, vol. 4, no. 3, pp. 621_645, 2012.

[13]O. Ali, A. Shrestha, J. Soar, and S. F. Wamba, ``Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review,'' Int. J. Inf. Manage., vol. 43, pp. 146_158, Dec. 2018.

[14] S. Camarasu-Pop, F. Cervenansky, Y. Cardenas, J.-Y. Nief, and H. Benoit-Cattin, ``Overview of medical data management solutions for research communities,'' in Proc. 10th IEEE/ACM Int. Conf. Cluster, Cloud
GridComput.,May2010,pp.739_744.

[15] M.BabithaandK.R.Babu,``Securecloudstorageusing AES encryption,'' in Proc. Int. Conf. Autom. Control Dyn. Optim. Techn. (ICACDOT), Sep. 2016, pp. 859_864.

[16]M. Sajjad, K. Muhammad, S. W. Baik, S. Rho, Z. Jan, S.-S. Yeo, and I. Mehmood, ``Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices,''MultimediaToolsAppl.,vol.76,no.3,pp.3519_3536,2017.

[17] M.Nofer,P.Gomber,O.Hinz,andD.Schiereck,
``Blockchain," Bus. Inf. Syst. Eng., vol. 59, no. 3, pp. 183_187, Mar. 2017.

[18]E. Yuan and J. Tong, ``Attributed based access control (ABAC) for web services," in Proc. IEEE Int. Conf. Web Services (ICWS), Jul. 2005,pp. 561_569.

[19] D. Mashima and M. Ahamad, ``Enhancing accountability of electronic health record usage via patient- centric monitoring," in Proc. 2nd ACM SIGHIT Symp. Int. Health Informat. (IHI), 2012, pp. 409_418.

[20] X. Sun, M. Li, H.Wang, and A. Plank, ``An ef_cient hash-based algorithm for minimal k-anonymity," in *Proc. 31st Australas. Conf. Comput. Sci.*, vol. 74, Jan. 2008, pp. 101_107.

[21] E. Kamalakannan and K. S. Arvind, ``Privacy conserving and secure distribution of personal health information using cloud," in *Proc. Int. Conf. Inf. Commun. Embedded Syst. (ICICES)*, Feb. 2014, pp. 1_4.

[22] P. Tasatanattakool and C. Techapanupreeda, ``User authentication algorithm with role-based access control for electronichealthsystemstopreventabuseofpatientprivacy," in *Proc. 3rd IEEE Int. Conf. Comput. Commun.(ICCC)*,Dec.2017,pp.1019_1024.

[23] C.Xu,J.Wang,L.Zhu,C.Zhang,andK.Sharif,
``PPMR: A privacy reserving online medical service recommendation scheme in Healthcare system,"*IEEE Internet Things J.*, vol. 6, no. 3, pp. 5665_5673, Jun. 2019.

[24] W.Liu,X.Liu,J.Liu,Q.Wu,J.Zhang,andY.Li,
``Auditing and revocation enabled role-based access control over outsourced private EHRs," in *Proc. IEEE 17th Int. Conf. High Perform. Comput. Commun. 7th Int. Symp. Cyberspace*