RESEARCH ARTICLE OPEN ACCESS

Data Integrity in Cloud Computing: A Revolutionary and Decentralized Perspective

Dr.M.Mohamed Ismail
Associate Professor
Department of Computer Science,
MazharulUloomCollege, Ambur, Tamil Nadu
hassimi@gmail.com

--************************----------------------------------

Abstract:
Cloud computing is a new computing model which enables individuals and organizations to gainaccess to huge computing resources without capital investment. It does mean that users can utilize computingresources in pay per use fashion. With virtualization technology the commoditization of computing resourceshas become a reality. The world is experiencing the advantages of cloud computing as industry giants likeMicrosoft, Google, Amazon etc. are providing cloud computing services. However, the cloud environment isconsidered in trusted as it is accessed through Internet. Therefore people have security concerns on datastorage security of cloud computing. Many techniques have been proposed in the literature for ensuring datastoragesecurityincloudcomputing.Thispaperpresentsthedetailsofthreemostrecenttechniquesthatcame into existence to protect clients data stored in cloud. The empirical results of these papers proved thattheyareeffectiveandcanbeusedinrealtimecloudcomputing.

***Keywords*—**Web Services, Virtualization, Cloud Computing

--************************----------------------------------

I. INTRODUCTION

With the advent of new technologies like Web Services and Virtualization, cloud computing became a reality.With cloud computing people can get three kinds of services such as platform as a service, software as a serviceand infrastructure as a service. The cloud deployment models include private cloud, public cloud, communitycloud and hybrid cloud. The private cloud is the cloud within an organization's network. Public cloud is thecloud accessible to entire world through internet based on certain standards. The community cloud is amongcompanies privately while the hybrid cloud is the combination of two or more types of cloud. As the cloud isbecomingmorepopular, therearegrowingsecurityconcerns.

These security concerns led to the research in the area and many researchers proposed protocols and techniquesto ensure cloud data security. The cloud service providers take care of compete security of cloud data. However,as the cloud is in trusted (accessed through Internet), lot of research went on storage security in cloud. Some ofthepapersandtheirtechniquesarebrieflyprovidedhere.In[1]distributedverificationprotocolsareinvented for ensuring data storage security in cloud computing. This is achieved by implementing a distributed auditingmechanism which ensures that the data dynamics of all cloud users are ensured and tested for integrity. In [2] athird party auditing mechanism is implemented in order to secure cloud storage. Continuous correctness of datais the SLA (Service Level Agreement) implemented in this paper. Public auditing of this paper helps in dataintegrity of multiple cloud users. In [3] a new approach is presented. It is known as distributed accountability fordata sharing. It is achieved by implementing a JAR which has data and security mechanism besides accessibilitylists for various cloud users. In [4] multi clouds are implemented in order to safeguard data of clients. In otherwords itis thecloudofcloudsforimprovingrobustnessofstorage security.

In [5] a novel approach is used to store, retrieve and forward data in the cloud. It uses secure erasure code toensure data security and encryption mechanisms for forwarding data to other legitimate users. In [6] cooperativeprovable data possessionconcept is used. It ensures that cloudenvironment works cooperatively and securedata. In [7] security to cloud data is provided using Sobol Sequence. This paper implemented a distributedverification protocol that relays on erasure code. In [8] also public auditing is implemented for cloud storagesecurity. The third party auditor checks for data integrity and ensures that the data is not tampered with in theserver. The rest of this paper is devoted to review three papers pertaining to data storage security problems incloud. Almost all papers assumed that, the cloud storage is not secure as the service provider may delete data orthecloudownerdoesnotdisclosestorageprobleminthecloud.

2. RelatedWorks

This section review literature of three most recent techniques that are used to ensure cloud data security. Eachtechnique is different from other technique. However, all the three techniques or approaches are meant forensuring data storage security in cloud computing. These three papers give enough insights into the storageproblems incloud,whicharerealorassumedandrequiredsecuritymeasures insomedetail.

2.1TowardSecureandDependableStorageServicesinCloudComputing

Cong Wang et al. [2] presented a mechanism for dependable and secure storage services that are meantfor cloud computing. The proposed mechanism in this paper allows cloud users to audit their data to preventclouddataproblems.Theauditingresultsreflectguaranteeofcloudstoragesecurity.

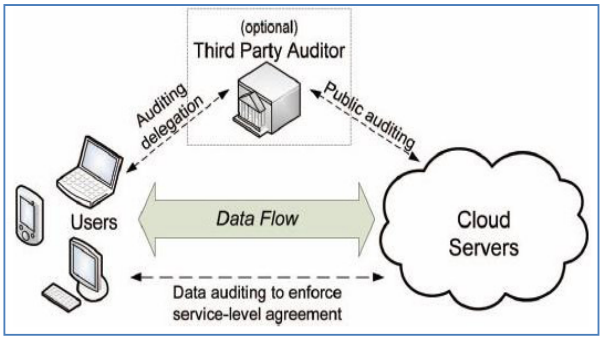

Fig.1–Architectureofcloudstorageservice[2]

From the above figure, it is evident that there are three parties involved. The users of cloud, the cloudservice provider and the third party auditor. Public auditing of cloud users data is the responsibility of TPA. Theusers of cloud delegate auditing job to TPA. This approach allows users of cloud to securely store data. It isachieved using encryptionin the form of a security setup module. Thendata canbe retrieved by users. It alsohasamechanismtoallowdatadynamicsthatareessential.Thisarchitectureachievessecurityusinghomomorphic tokens and also the distributed erasure coded data. The adversary model used in this papercapturesvariouskindsofsecuritythreats.Itusessomeapproachessuchasfiledistributionpreparation,challenge token precomputation, and correctness verification [2]. The data auditing helps the data owners to feelgood as it proves the integrity of data. Here the service level agreement is nothing but the agreement betweenparties. For instance, in this paper, the SLA on the continuous data integrity of the cloud storage is one of theservice level agreements. The moment the integrity of data is lost and verified, and then it does mean that thereare inconstancies in the cloud storage. To avoid such inconsistencies and ensure that data ownersgain inconfidenceoncloudstoragethispaperincludingotherscameintoexistence.

3.ExperimentsandFutureWork

Experiments are made on various aspects using auditing scheme. The proposed work in this paper is meant forsecuring cloud data. Towards, it implemented mechanisms that support storage, retrieval, and data dynamicssuch as update, delete and append operations. Performance is evaluated in terms of file distribution propagation,challenge token recomputationetc [2]. Here the data is divided into blocks, encrypted and stored in cloudstorage.Thusitgivessecurity.Thispaperdid notgiveanydirectionsforfuturework.However,thispapercanbe extendedby implementing more service levelagreements and also letting the serverto keeptrackofmisbehavingnodes.

4.EnsuringDistributedAccountabilityforDataSharingintheCloud

SmithaSundareswaranandSquicciarini[3]proposed anew cloudstorage modelthatensures distributedaccountability. The proposed framework is an object oriented solution that leverages JAR programming forensuring data security. It exploits JAR's programming capabilities. Besides this, this paper also uses distributedauditing mechanism. The security mechanism involves data owner, cloud service provider, certificate authority,and JAR entity. JAR is programmable and dynamic. JAR stands for Java Archive. The JARS are possible withvarious extensions in Java. For instance .jarfiles forstoring data in compressed format. Data owners aresupposed to create a JAR file which contains data as well as security mechanisms. Such JAR is kept in cloud forscalabilityreasons[3].Fig.2showsoverviewofthisapproach.

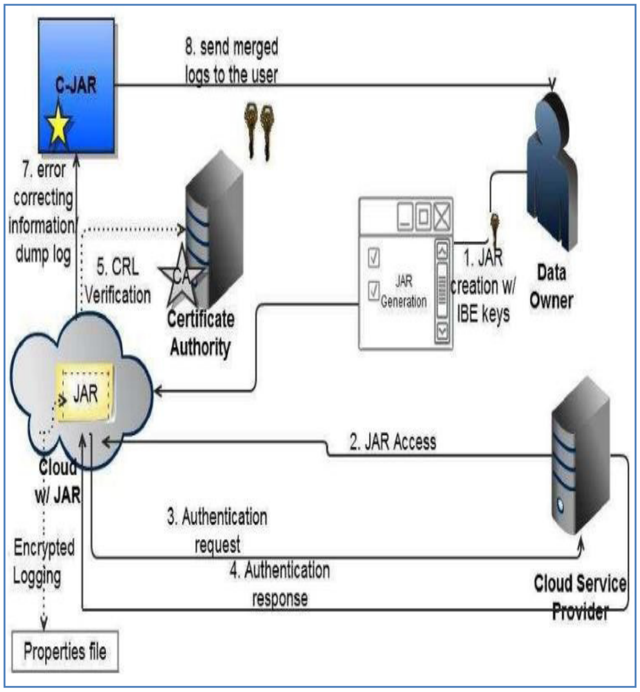

Fig.2–Distributed AccountabilityFramework[3]

As can be seen in fig. 2, it is evident that the security mechanism is distributed in nature. First of all thedataownercreatesaJARfilewhichencapsulatesotherJARfileswithdataandencryption,decryptionmechanisms. The JARs are nested. The outer JAR is responsible for authentication while the inner jars containactual data inencryptedformat and also cryptographic mechanisms.Aftercreating the JAR the data ownerkeeps that JAR in cloud [3]. The cloud service provider and other users can access it from cloud based on theirprivileges and accessibility privileges. This is a secure mechanism that prevents data inconsistency, privacy,confidentialityandothersecurityproblems[3].Acertificateauthorityisalsoinvolvedinthesecurity mechanisms. The CA is responsible for providing digital certificates to the participants. These digital certificateswill help the candidates or parties to prove themselves as they contain identity of the people. This framework issupporting encryptedlogging.Logging doesmean recordingevents. The events are recorded as they happen.The logging data is encrypted first and logged for security reasons. With regard to encryption when data ownercreates JAR file, the data being stored is encrypted and kept in an inner JAR file. The decryption takes placewhen the JAR is accessed by an authorized user [3]. Complete log information is provided to the data ownerfromtimetotime.Variouskinds oflogfiles aremergedintoasingleoneandsenttothedataowner[3].

5.ExperimentalResultsandFutureWork

Using Emulabtestbed the proposed framework is tested. The environments include open SSL servers. Theexperimental results reveal that the proposed framework is very secure and integrity of data can be preventedstrictly. There are many experiments done for knowing its performance. For instance log creation time, loggingtime, log merging time, authentication time etc. areexperimented using profiling. The results reveal thattheframework is computationally viable. The authors provided directions for future work i.e. to refine the presentapproachbyverifyingtheJVMandJREatruntimebesidesauthenticatingtheJARs.

The future research focuses on developing tamper resistant applications that work with complete security. Suchapplicationsareinherentlysecureandtheadversariescan'tbreakthesecurityofsuchapplications[3].

6. ASecureErasureCode-BasedCloudStorageSystem withSecure DataForwarding

Hsiao-Ying Lin and Wen-GueyTzeng [5] proposed a new secure storage mechanism forcloud. The newframework is based on securer erasure codes. The proposed system allows data owner to perform secure datastorage, secure retrieval of data and secure data forwarding. It has robust mechanisms for storing data and alsosecuring the data. The server side environment has both storage servers and security servers. The storage serversare responsible to store data inencryptedformat while the security serversorkey serversare meant formaintainingsecuritykeysandinvolvinginauthenticationandauthorizationmechanisms.Thesecuritymechanism is based on proxy re-encryption scheme. The decentralized erasure code pertaining to cloud data isintegrated with distributed storage system. The key features of this paper is that the proxy re-encryption scheme.This scheme enables encoding operations on already encrypted data and also let the user to forward it to otherusersusingpublickeycryptography[5].

Public key cryptography is the asymmetric cryptography which does not involve in exchange of privatekeys. In this approach every participant has a public key and private key combination. The public key is knownto all partners while the private key is kept secret. When a person sends data to other person by decryption themessage with the public key of the recipient, only the private key of the recipient is allowed to decrypt it. Thismechanismisused forsecuredataforwarding.Fig.3showstheproposedsystemanditsarchitecture[5].

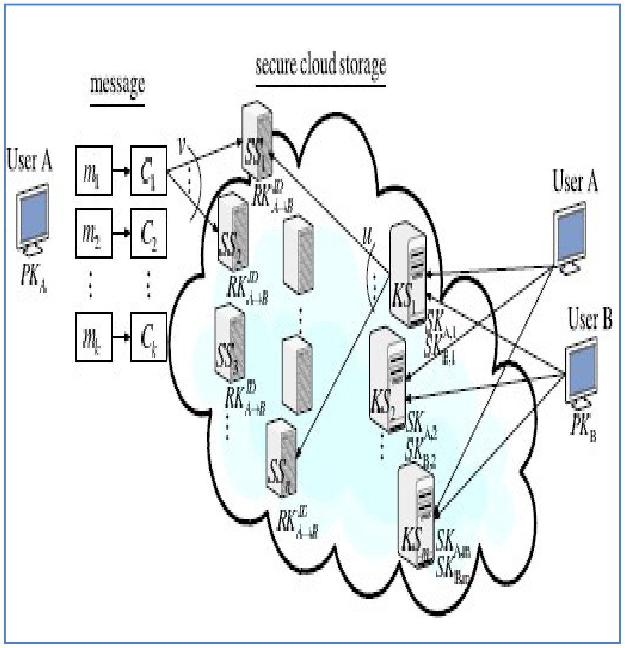

Fig.3–SecureCloudStoragerchitecture[5]

As can be seen in fig. 3, the data owner takes a file and divides it into many blocks such as m1, m2, etc.Each block is further subjected to encryption. The result is cipher text represented by c1, c2, etc. The cipher textis then stored in multiple storage servers. Before performing storage, the user has to do generate keys which arestored in Key Servers. The Key Servers are meant for storing security keys while the storage servers. When dataowner wants to retrieve data, then the key servers have to authenticate him and the storage servers take theresponsibility of storing data securely. Therefore, the storage and retrieval operations are carried out by dataowner. On the other hand, the data forwarding is supported by the framework. In case of data forwarding, thedataownergivesinstructions to cloudstorage to forward so and so message to otheruser. Thenthe cloudservers willdoactualforwardingusingpublickeyencryption.

6.1ExperimentalResultsandFutureWork

Experimentsaremadeusingtheproposedframework intermsofstoringdata,retrievingdataandalsoforwarding data. The experiments are intended to evaluate the system in terms of security, correctness andcomputational complexities. The experimental results reveal that the system is computationally feasible andprovides secureenvironmentwithdataretrieval,datastorageanddataforwardingprovisions.

Conclusion

This paperpresents, the three most recent techniques thatcame into existence,to implement data storagesecurity in cloud computing. All the papers have provided different architectural framework to ensure the datasecurity incloudstorage. This is required as the cloudis considered intrusted. The first paper has focusedonthe auditing mechanism for cloud security. The second paper focused on the distributed accountability of cloudstorage.InthispaperaJARprogrammingmodel hasbeenleveragedinordertoaccommodatesecurityprimitives in a distributed environment. It contains features like secure logging, secure data retrieval as per theprivileges or access rights given.The third paper focused on the erasure code based cloud security with twotypes of servers namely storage servers and key servers.This has got more sophisticated security withsupportfordatastoragedataretrievalandsecuredataforwarding.

References

[1] DistributedVerificationProtocolsforDataStorageSecurityinCloudComputingPriodyuti Pradhan,P.SyamKumar,GautamMahapatra, R.Subramanian2012InternationalConferenceonCommunication,Information&ComputingTechnology(ICCICT),Oct. 19-20,Mumbai,India.

[2] Toward Secure and Dependable Storage Services in Cloud ComputingCong Wang

Qian WangKuiRenNing Cao, WenjingLouIEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. 5, NO. 2,APRIL-JUNE2012.

[3] EnsuringDistributedAccountabilityforDataSharingintheCloudSmithaSundareswaran,Anna

[4] C. Squicciarini IEEE TRANSACTIONS ON DEPENDABLE AND SECURECOMPUTING, VOL. 9, NO. 4,JULY/AUGUST2012.

[5] Cloud Computing Security: From Single to Multi-Clouds Mohammed A. AlZain , Eric Pardede ,BenSoh,James A.Thom201245th HawaiiInternationalConferenceonSystemSciences.

[6] A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding Hsiao-YingLinWen-GueyTzeng IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23,NO.6,JUNE2012.

[7] CooperativeProvable Data Possession forIntegrity Verification in Multi-Cloud Storage YanZhu, Hongxin Hu, Gail-JoonAhnMengyang IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTEDSYSTEMS.

[8] Ensuring Data Storage Security in Cloud Computing using Sobol SequenceP. Syam Kumar, R.Subramanian and D. ThamizhSelvam2010 1st International Conference on Parallel, Distributed and GridComputing(PDGC-2010).

[9] Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing Cong Wang,QianWang,andKuiRenWenjingLouIEEECommunicationsSocietyIEEEINFOCOM2010.