Journal of Vibration Engineering

Registered

Our Website
www.jove.science

Implementing SecureDataStorage andSharingTechniquesforadvancedProtectionsin CloudEnvironments

[1]Ms.SmitaB.Zanke,[2]Prof.C.M.Mankar

[1]Student,DepartmentofComputerScienceandEngineering

[2]AssistantProfessor,DepartmentofComputerScienceandEngineering,

[1][2]ShriSantGajananMaharajCollegeofEngineering,Shegaon.

Abstract:

Cloud computing has gained a lot of hype in the current world of I.T. Cloud computing is said to bethe next big thing in the computer world after the internet. Cloud computing is the use of theInternet for the tasks performed on the computer and it is visualized as the next-generationarchitecture of IT Enterprise. The 'Cloud' represents the internet. Cloud computing is related toseveral technologies and the convergence of various technologies has emerged to be called cloudcomputing. In comparison to conventional ways Cloud Computing moves application software anddatabasestothelargedatacenters,wherethedataandserviceswillnotbefullytrustworthy.Inthisarticle, I focus on secure data storage in cloud; it is an important aspect of Quality of Service. Toensurethecorrectnessofusers'datainthecloud,Iproposeaneffectualandadaptableschemewithsalientqualities.Thisschemeachievesthedatastoragecorrectness,allowtheauthenticatedusertoaccessthedataanddataerrorlocalization,i.e.,theidentificationofmisbehavingservers.

Keywords:Computing,virtualization,grid,computations,applications

1. Introduction

The most popular advanced technology in use now is cloud computing. Being an Internet-basedcomputer technology, cloud computing. The "CLOUD" has been deployed by some of the biggestcompanies, like Amazon, Microsoft, and Google, which have been employing it to accelerate theiroperations. The whole outsourcing industry (SaaS, PaaS, and IaaS) has taken on a new dimensionthanks to cloud computing, which also offers ever-cheaper, more potent processors with variouscomputing architectures. A computer's most basic function is to store information in the availablespace and retrieve it whenever the registered user requests it. Any type of data that we use everyday may be stored, including basic pictures, our favourite tunes, saved movies, vast quantities ofsecret data, and even little amounts of data. The most fundamental service provided by cloudcomputingistheonejustdescribed.

Cloud is a pool of computing service on large scale. The increasing network bandwidth and reliableyet flexible network connections make it even possible that users can now subscribe high qualityservicesfromdataandsoftwarethatresidesolelyonremotedatacenters.TheCloudhelpsenterprises to have a dynamically scalable abstracted computing infrastructure that is available on-demand and on a pay-per-use basis. This model not only saves the IT teams from investing heavilyon infrastructure, but also shields them from the intricacies involved in infrastructure setup andmanagement.Presently,apartfromprovidingtheon-demandITinfrastructure,cloudserviceproviderstypicallyprovideinterfacesforotherrelatedITmanagementservices.Cloudbasedflexibleandondemandinfrastructureenablesatravelenterprisetooffermobilityandsocialmediachannelswithout incurring any fixed cost. Using a cloud infrastructure, a travel enterprise can start in a smallwayandgrowintotheseevolvingmarketswithalowerriskandfinancialstrain.Fromtheperspectiveofdatasecurity,whichhas alwaysbeenanimportantaspectofqualityofservice,CloudComputinginevitablyposesnewchallengingsecuritythreatsfornumberofreasons.Atfirst,traditional cryptographic primitives for the purpose of data security protection can not be directlyadopted due to the users' loss control of data under Cloud Computing. Therefore, we requireverificationofdatastorageinthecloud.Consideringvariouskindsofdataforeachuserstoredinthecloudandthedemandoflongtermcontinuousassuranceoftheirdatasafety,theproblemof

verifying accuracy of data storage in the cloud becomes even more challenging. Secondly, CloudComputingisnotjustathirdpartydatawarehouse.

The stored data in cloud may be frequently revised by the users, including operations like insertion,deletion, modification, affixing, reordering, etc. To ensure storage correctness under dynamic datarevise is hence of paramount importance. However, this dynamic feature also makes traditionalintegrityinsurancetechniquesfutileandentailsnewsolutions.ThedeploymentofCloudComputingispoweredbydatacentersrunninginasimultaneous,cooperatedanddistributedmanner.Individual user's data is redundantly stored in multiple physical locations to further reduce the dataintegritythreats.

Ensuring storage correctness without having users possessing data, cannot address all the securitythreats in cloud data storage, since they are all focusing on single server scenario and most of themdonotconsiderdynamicdataoperations.Thisisconqueredusingdistributedprotocolsforensurings torage correctness across multiple servers or peers. In this paper, we propose an effective andflexible scheme with explicit dynamic data support to ensure the correctness of users' data in thecloud.Werelyonerasure-correctingcodeinthefiledistributionpreparationtoprovideredundanciesandguaranteethedatadepend ability.Thisconstructiondrasticallyreducesthecommunicationandstorageoverheadascomparedtothe traditionalreplication-basedfiledistribution techniques. By utilizing this token with distributed verification of erasure-coded data,our scheme achieves the storage correctness insurance as well as data error localization. ErrorLocalizationisthedatacorruptionthathasbeendetecteddduringthestoragecorrectnessverification, our scheme can almost guarantee the simultaneous localization of data errors, i.e., theidentificationofthemisbehavingserver(s).

ThisisamongfirstfewonesinthisfieldtoconsiderdistributeddatastorageinCloudComputing.Themainco ntributioncanberecapitulatedasthefollowingaspects:

When compared to its predecessors they only provide binary results about the data storage statusacross the distributed servers, the protocol used in our work provides point of data error (i.e. ErrorLocalization).

- Weprovidesecureandefficientdynamicoperationsondatablocks.
- The security and performance analysis shows the proposed scheme is highly efficient andresilientagainstByzantinefailure,maliciousdata modificationattack,andevenservercolludingattacks.

In cloud data storage system, users store their data in the cloud and no longer possess the datalocally. Thus, the correctness and availability of the data files being stored on the distributed cloudservers must be guaranteed. One of the key issues is to effectively detect any unauthorized datamodification and corruption, possibly due to server compromise and/or random Byzantine failures.Besides, in the distributed case when such inconsistencies are successfully detected, to find whichserver the data error lies in is also of great significance, since it can be the first step to fast recoverthe storage errors. To address these problems, our main scheme for ensuring cloud data storage ispresented in this section. The first part of the section is devoted to a review of basic tools fromcoding theory that are needed in our scheme for file distribution across cloud servers. Then, thehomomorphictokenisintroduced.Thetokencomputationfunctionweareconsideringbelongstoafa mily of universal hash function, chosen to preserve the homomorphic properties, which can beperfectlyintegratedwiththeverificationoferasurecodeddata.

2. LiteratureSurvey

Mendonca S [1] stated that SaaS, PaaS, and IaaS are the three services that cloud computing offerstothecustomer. Differentlevels ofsecurityare offeredin thecloud computing environmentthrough these service models. Data security, data integrity, identity management, data location,data availability, and other factors need to be taken into consideration for better data security incloud computing in order to have a secured cloud computing environment and to speed up cloudelementsinSaaSservicemodel.

- Data Security and Data Protection – Once the client uploads data to the cloud, there shouldbesomeassurancethat access willonly be permitted bythose whohave been givenpermission. Another risk that could potentially endanger cloud data is improper access tocustomersensitivedata bycloudstaff.

- Data Integrity- Cloud service providers should put in place methods to assure data integrityand be able to explain what happened to a specific dataset and when. This is done byoffering data security. It might be important to keep detailed records of the data that wasstoredin apublic cloud.When such requirementsfordata integrity arepresent, itisnecessarytoretaintheoriginandcustodyofdataorinformationinordertostoptamperingwithi torexposingitoutsideofthepredeterminedboundaries.

- Datalocalizationandrelocationaremadepossibleviacloudcomputing.Consumersfrequently have no idea where their data is located. An organisation may wish to knowwheretheirsensitivedataissecurelystoredifitiskeptonacloud-basedstoragedevice.Thiscallsforacontractbetweenthecloudserviceproviderandtheclientspe cifyingthelocationor server where the data shall remain. on order to secure the data on the cloud, it isfrequentlymovedfromonelocationtoanother.SLAs(ServiceLevelAgreements)arecontractsb etweencloudserviceprovidersthatallowthemtoshareresources.

- Data Availability: Typically, customer data is stored in segments on various servers spreadacrossvariouslocationsoronvariousclouds.Astheavailabilityofseamlessanduninterrupt ibleprovisionbecomesmorechallenginginthissituation,dataavailabilitybecomesaseriousprobl em.Therefore,itiscrucialthatthesuppliergivetheauthoriseduserproperaccesstothedata.

- Identity Management – Each user must authenticate themselves in order to access cloudservices.Forthepurposeofprovidingauthenticationandauthorization,theprovidershould offer an identity management system. This is a significant concern in a cloud computingenvironmentforboththeproviderandtheuser.[1]

Pan Yang [2] mentioned that as the Internet of Things (IoT) gains popularity, more information-sensing gadgets are becoming online in order to realise how interconnected people, gadgets, and"things" are. According to a recent forecast from IDC, there will be 41.6 billion internet of things(IoT)"things"in2025,producing79.4zettabytes(ZB)ofdata.Additionally,peoplearestilldedicatedt o enhancing the effectiveness of data collecting from IoT devices. The cloud service providerplatform generates and hosts an unprecedented volume of data. Numerous smart city apps andserviceswillbehousedinthecloudduetoitshighperformance,scalable,andstabledatacenters.Inorde r to host, develop, and/or launch their smart city services and apps, citizens of smart cities andservice providers can rely on cloud services. Additionally, the benefit of pay-as-you-go forces themajority of conventional organisations to actively shift data to the cloud. The cloud not only hostsworkloads but also offers effective operational procedures, enhancing the flexibility and agility ofbusinesses. Both enterprise digital transformation and network modernization transformation havebenefited from this. The United Nations' 2019 Digital Economy Report emphasises how the digitaleconomy is evolving into a significant engine for economic growth. Statistics are not complete,howeverthedigitaleconomymakesup4.5%to15.5%ofglobalGDP.Cloudcomputingisessentia ltoexpediting the development of the modern economic system and promotes the deep integration oftheInternet,bigdata,artificialintelligence,andtherealeconomy.Theglobalmarketforpublic

cloudserviceswillincreaseby17%to$266.4billionin2020from$227.8billionin2019,predictsGartner,Inc..Collectively,cloudapplicationscontinuetobepopular.[2]

Salim et. Al [3] Cloud computing is a new technology often used virtualized with resources toprovidedynamicallyscalableserviceviatheinternet.Inthecloudcomputing,userscanaccesstotheresources by using a various devices, such as laptops, PCs, smart phone, etc. to access multipleservicesuchasstorage,programs,andapplication-developmentplatforms,overservicethatprovided by cloud providers via the internet. Through the last years, Cloud computing improvedfromsimplewebapplications,suchasGmailandHotmail,intobusinesspropositionslikeSalesForce.com, AmazonEC2, etc. Cloud computing may be supply service for reducing IT costs,business management, and maintenance costs of hardware and software are effective. At the sametime, it makes the enterprises able to access to professional IT solutions. Data storage center incloud computing can be reliable and secure, because the world's most advance data center ishelping the users save the data. The users must not concern about virus attack, data loss, and otherproblems when they used the cloud in correct form. User with cloud computing can use the cloudservices anywhere, everywhere, on-demand and based on pay per use principle. Cloud computinghas two types of models: services models (SaaS, PaaS, and IaaS), and deployment models (Public,Private,Community,andHybridcloud).Alsothecloudcomputingiscontainsfiveessentialcharacteristics(On-Demand,BroadNetworkAccess,RapidElasticity,MeasuredService,andResourcepooling).ThereareманycompaniesthatprovidecloudservicessuchasAmazon,Google,Microsoft,and SalesForce.com, etc. There are many concerns about the data security in cloud computingshould be taken into account such as violation of the confidentiality and privacy of customers' datavia unauthorized parties. The major concern is if data secure when it save in cloud?. Therefore, wehave dedicated our work to design a new architecture to improve data security in cloud computingby using modified Identity-Based Cryptography (MIBC) and Elliptic Curve Integrated EncryptionScheme(ECIES)Algorithm.

Vamseek[4]proposedplayfairandvigenereciphertechniquesthatweremergedwithstructuralaspectsofSimplifiedDataEncryptionStandard(SDES)andDataEncryptionStandard(DES).Inwhich64 bit block size of plain text is taken which is fixedand this 64 bit plain text is divided into twohalves by using the "black box" the right half have 2 bits whereas left half has6 bits, then these 6bits are feed into "superior function" block where these 6 bits are further separated intwo halveswhere first two bits represent the rows and last four bits represent the columnby identifying therowsandcolumnthecorrespondingvaluecanbeselected.Thenthisfunctionisaplliedtoall8octetsof the output of vigenere block the resultant of black box is againof 64 bits then these bits arefurther divided into 4 new octants similarly right 4 bits are unified to formulate right halves. Finallyleft and right halves are XOR-ed toobtain left half of this arrangement. This process is repeatedthreetimes.

Shuai, H., & Jianchuan, X [5] worked with RSA algorithm to encrypt the data and BilinearDiffie-Hellman to insure the security while exchanging the keys. In proposed method a message header isadded in front of each data packet for direct and safe communicationbetween client and cloudwithout any third party server. When user sends the request to the cloud server for data storagethen cloud server creates the user public key, private key and useridentification in certain server.Two tasks performed at user end before sending the file to cloud, first add message header to thedata and secondly encrypt data including message header by using secret key. When user requestfor data to the cloud server then it will check the message header of received data and pick up theUniqueIdentificationforServerincloud(SID)information.IfSIDinformationisfounditwillrespondtheuserrequestotherwiserequestwillbediscarded.

Sood,S.K.[6]usedintroducedatechniquetoensuretheavailability,integrityandconfidentialityofdata incloudbyusingSecureSocketLayer(SSL)128bitencryptionthatcanalsoberaisedto256bitencryption.Th euserwhowishestoaccessthedatafromcloudisstrictlyrequiredtoprovidevaliduseridentityandpasswor dbeforeaccessisgiventotheencrypteddata.

Parsi Kalpana [7] worked with user module to send the data to the cloud then cloud serviceprovider generate a key and encrypts the user data by using RSA algorithm and stored the data intoits data centre. When user request the data from cloud then cloud service provider verify theauthenticityoftheuserandgivetheencrypteddatatotheuserthatcanbedecryptedbycalculatingthep rivatekey.

Mohamed, E. M., Abdelkader [8] developed a three layered data security model is presented inwhich each layer performs different task to make the data secure in cloud. First layer is responsiblefor authentication,second layer performs the duty of data encryption and third layer performs thefunctionalityofdatarecovery.

Singh, J., Kumar, B., & Khatri [9] used RC5 algorithm that is implemented to secure the data incloud.Anencrypteddataistransmittedevenifthedataisstolentherewillbenocorrespondingkeyto decryptthedata.

Lan, Z., Varadharajan [10] developed a Role Base Encryption (RBE) technique that is proposed tosecure the data in cloud and role base access control (RBAC) cloud architecture was also proposedwhich allows organizations to store data securely in public cloud, while maintaining the secretinformationoforganization'sstructureinprivatecloud.

3. ProblemStatement

Future-generation technology for IT businesses is cloud computing. It offers several variousqualities,includingscalability,multi-
user,virtualization,andmanymore.Aswellprovidescomputational infrastructure that is available on demand, which has the ability to lower the cost ofdeveloping IT-based services. It is capable of offering a variety of services online. The ability forcustomerstostoretheirdataasneededisoneofthekeyservicesofferedbythecloud.Theuserhasa
difficult situation because all the data are stored in a global resource pool that is interconnectedbutdispersedamongmanylocations.Thesedatacouldbeaccessedbyanunauthoriseduse rviathevirtualmachines.Thisisthenegativeaspectofclouddatastorage.Usersfaceaseriousdifficultyasar esult of this insecurity. As a result, a significant issue with cloud computing is data security. AES iscurrently thought to be the most well-liked symmetric cryptographic method[11-12]. It is crucial tocreatehigh-
performanceAESinordertoincreasethescopeofitsgeneraluse.Andhencethefurthersecurityofencrypte ddataisnecessarytosecuredoncloud.

4. Objectives
- Toimplementtwostepofencryptionprocedure
- ToAuthenticatecloudenvironmentwithconsideringhighriskassessment
- Toresolvemaximumissuerelatedtodataleakagewhilestoringthedataincloud

5. ProposedMethodology

5.1 TwoLevelCryptographictechniquesusingAESandECCAlgorithm

- **Input**:

  Inthisstep,usercansendtheoriginaldataormessage.
- **Encryption**:

  Step1:Here,wecanencrypttheoriginalmessageordatabyusingAESalgorithm.Step2:Generateasecretkey.

  Step3:Secondlevel,againwecanencryptthedatabyusingECCalgorithm[13].
- **Storage**:Here,wecanstoretheencrypteddataincloudformoresecurity(Boxcloudorcloudme)
- **Decryption**:

  Step1:Here,wecandecrypttheencrypteddatabyusinggeneratedkey.
- **Performance**:Here,wecanestimatesomeperformancemetricssuchas
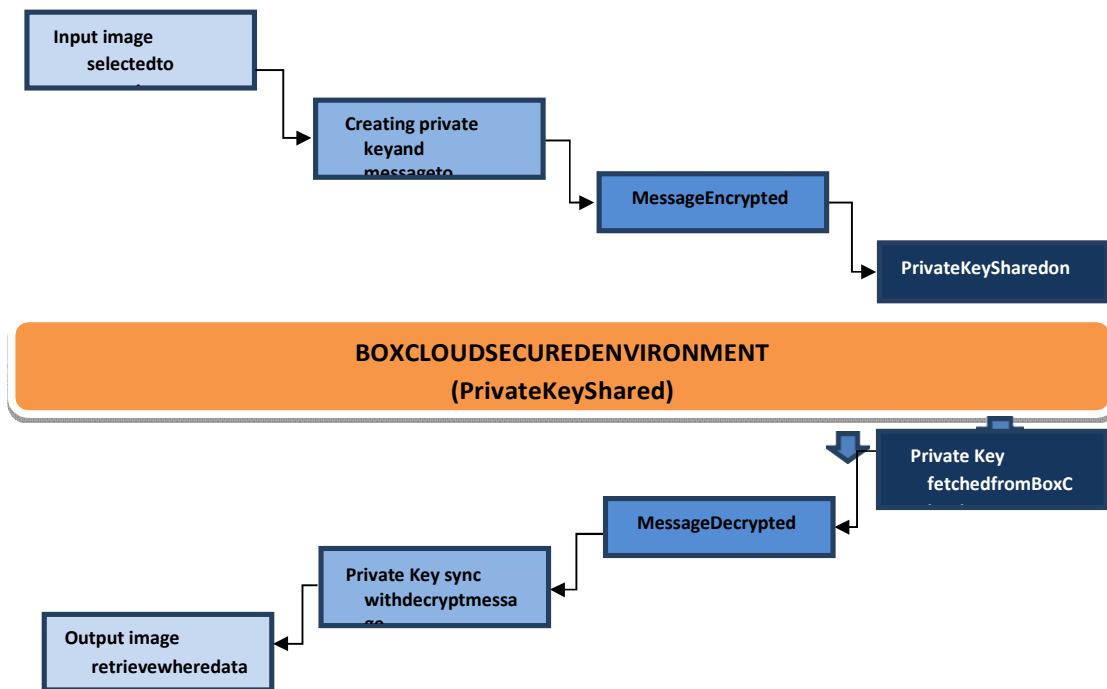 - PSNR
  - MSE

7. Proposedflowofthesystem
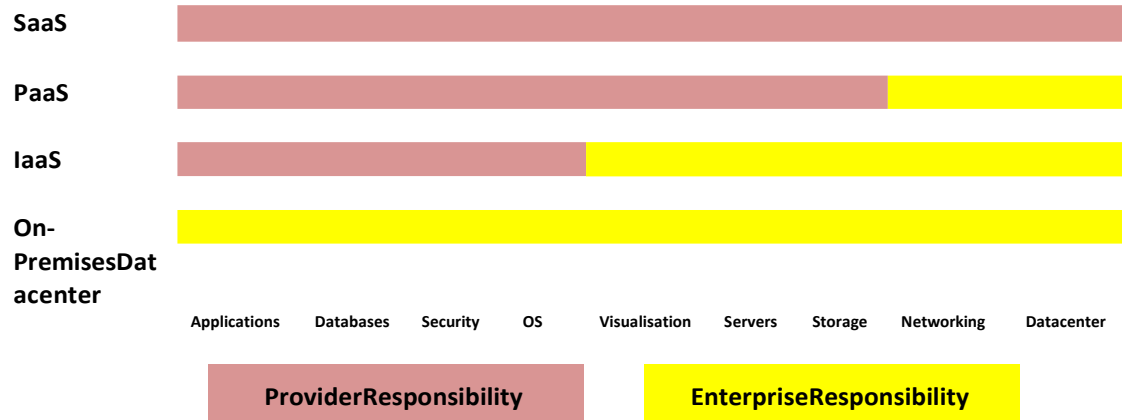

Fig.1.Flowdiagramoftheproposedprocess

Fig.2ComparisonofresponsibilitiesofCloudComputingenvironmentinvariousfields
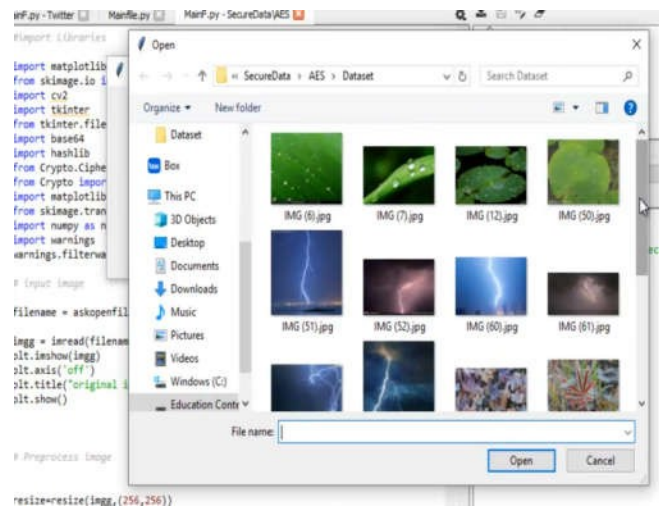
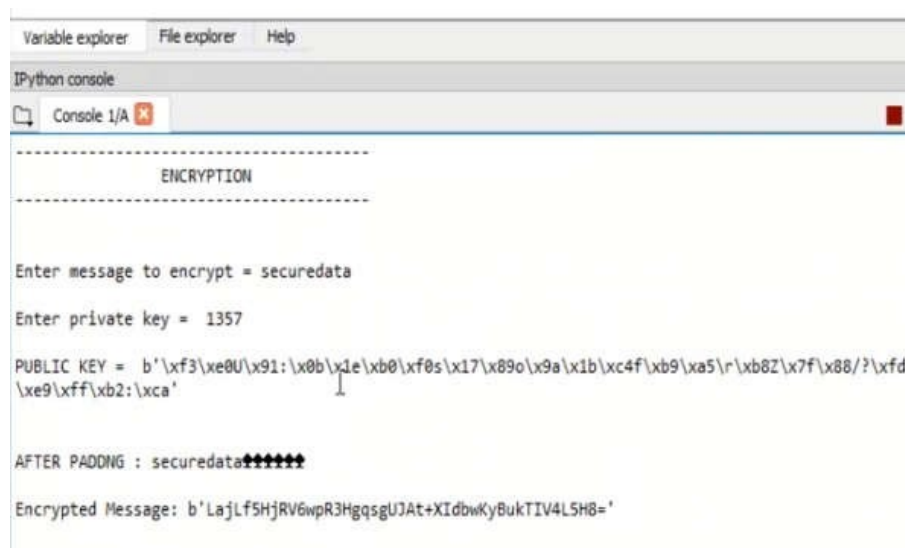## 8. Implementation

Fig.3Editorwindowandselectionofdata

Fig.4Messagetoencryptandprivatekeysavingonboxcloud

Fig.5.Decryptionandfetchingprivatekeyfromboxcloud

Fig.6.PerformanceEstimation

9. ObjectiveandvariousTechnicalMethodsforSecurityFeaturesincloudObjective1

Collaborativeaccesscontrol
ProposedSchemes: Attribute-basedcontrolled,collaborativeaccesscontrolscheme
TechnicalMethods: Translationnodesinsertion,Dataconfidentiality[14]

Objective2
Self-adaptiveaccesscontrol
ProposedSchemes: Self-adaptiveaccesscontrolwithsmartdeduplication[15]
TechnicalMethods: Break-glassaccess,Securededuplication,Dataconfidentiality,Securededuplication

Objective3
Group-orientedaccesscontrol
ProposedSchemes: Attribute-basedprivacy-preservingdatasharingfordynamicgroups
TechnicalMethods: Broadcastencryption,Re-encryptionalgorithms,Dataconfidentiality,Fine-grainedaccesscontrol, Dynamicgroupsdatasharing

10.Conclusion

A literature review of the works in the area of cloud computing data security is conducted and theresults of review are presented in this paper. The results show that the majority of approaches arebased on encryption (45%) out of which 71% encryption techniques results are validated. 67% ofencryptiontechniquesusedexperimentationtovalidatetheresults.Theseresultspointtowardsthefact thatmostofresearchersshowtheirinterestinencryptiontechniquetoenhance thesecurityof

data in cloud computing environment. The results also reveals the fact of lack of validation inproposedapproachesas42%ofthestudiesprovidenovalidationoftheresultsoutofwhich67%areguidel ines.Onlyfewstudieshaveusedstatisticalanalysisforvalidation.Thisarea(validation)needstheattention oftheresearchcommunitytogainthetrustandconfidenceofcloudcomputingusers.

References:

[1] SmithaNishaMendonca,"DataSecurityinCloudusingAES",InternationalJournalofEngineeringResearch&Tec hnology(IJERT)http://www.ijert.orgISSN:2278-0181IJERTV7IS010104Vol.7Issue01, January-2018

[2] Pan Yang1, Neal N. Xiong2, And Jingli Ren1," Data Security and Privacy Protection for Cloud Storage: ASurvey",10.1109/ACCESS.2020.3009876,IEEEAccess,Volume4,2016

[3] Salim Ali Abbas, Amal Abdul Baqi Maryoosh," Data Security for Cloud Computing based on Elliptic CurveIntegrated Encryption Scheme (ECIES) and Modified Identity based Cryptography (MIBC)", InternationalJournalofAppliedInformationSystems(IJAIS)–ISSN:2249- 0868FoundationofComputerScienceFCS, NewYork,USAVolume10–No.6,March2016

[4] Vamseekandsriramr,(2011)"DataSecurityinCloudComputing,"inJournalofComputerandMathematicalScie ncesVol.2, pp.1-169

[5] Shuai, H., & Jianchuan, X. (2011, 15-17 Sept. 2011). Ensuring data storage security through a novel thirdparty auditor scheme in cloud computing. Paper presented at the Cloud Computing and IntelligenceSystems(CCIS),2011IEEEInternational Conferenceon.

[6] Sood, S. K. (2012). A combined approach to ensure data security in cloud computing. Journal of Networkand ComputerApplications, 35(6),1831- 1838

[7] ParsiKalpana&SudhaSingaraju(2012).DataSecurityinCloudComputingusingRSAAlgorithm.InternationalJour nalofResearchinComputerandCommunicationtechnology(IJRCCT),vol1,Issue4.

[8] Mohamed, E. M., Abdelkader, H. S., & El-Etriby, S. (2012,14-16 May 2012). Enhanced data security modelfor cloud computing. Paper presented at the Informatics and Systems (INFOS), 2012 8th InternationalConferenceon.

[9] Singh, J., Kumar, B., & Khatri, A. (2012, 6-8 Dec. 2012). Improving stored data security in Cloud using Rc5algorithm.PaperpresentedattheEngineering(NUiCONE),2012NirmaUniversityInternationalConference on.

[10] Lan,Z.,Varadharajan,V.,&Hitchens,M.(2013).AchievingSecureRole-BasedAccessControlonEncrypted   Data in Cloud Storage. Information Forensics and Security, IEEE Transactions on, 8(12), 1947-1960.

[11] Taeho, J., Xiang-Yang, L., Zhiguo, W., & Meng, W. (2013, 14-19 April 2013). Privacy preserving cloud dataaccesswithmulti-authorities. PaperpresentedattheINFOCOM, 2013Proceedings IEEE

[12] Ravindra Changala, "Secured Activity Based Authentication System", Journal of innovations in computerscienceandengineering(JICSE),Volume6,Issue1,Pages1-4,September2016.ISSN:2455-3506.

[13] Ishu Gupta, "Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments: ASystematicReview,Analysis,andFutureDirections",VOLUME10,2022,IEEEAccess.

[14] MazharAli,"SeDaSC:Securedatasharinginclouds",1932-8184©2015IEEE.

[15] CloudsecurityAlliance,"Securityguidelinesforcriticalareasoffocusincloudcomputingv3.0,"2011.