International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 143-153 www.ijaem.net ISSN: 2395-5252

Data Security and Privacy in Cloud Computing SAM College of Engineering and Technology, Bhopal, Madhya Pradesh

Mr Navneet Singh Khurana,
Corresponding Author: Prof . Ankur Thaneja

Submitted: 25-02-2021 Revised: 05-03-2021 Accepted: 10-03-2021

ABSTRACT: Data security has consistently been a major issue in information technology. In the cloud computing environment, it becomes particularly serious because the data is located in different places even in all the globe. Data security and privacy protection are the two main factors of user's concerns about the cloud technology. Though many techniques on the topics in cloud computing havebeeninvestigatedinbothacademicsandindustries ,datasecurityandprivacyprotectionarebecomingmor eimportantforthe future development of cloud computing technology in government, industry, and business. Data security and privacy protection issuesarerelevanttobothhardwareandsoftwareinthecl oudarchitecture.Thisstudyistoreviewdifferentsecurit ytechniquesand challenges from both software and hardware aspects for protecting data in the cloud and aims at enhancing the data security and privacy protection for the trustworthy cloud environment. In this paper, we make a comparative research analysis of the existing researchworkregardingthedatasecurityandprivacypr otectiontechniquesusedinthecloudcomputing.

I. INTRODUCTION

Cloud computing has been envisioned as the next gener- ation paradigm in computation. In the cloud computing environment, both applications and resources are delivered on demand over the Internet as services. Cloud is an environment of the hardware and software resources in the data centersthatprovidediverseservicesoverthenetworkor the Internet to satisfy user's requirements[1]. Theexplanationof"cloudcomputing"fromtheNationa l Institute of Standards and Technology (NIST) [2] is that cloud computing enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources(e.g.,networks,servers,storage,applications ,and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. According to the explanation, cloud computing provides a convenient on-demand network access to a shared pool of configurable computing resources. Resources refer to com- puting applications, network resources, platforms, software services, virtual servers, and computinginfrastructure.

Cloudcomputingcanbeconsideredasanewc omputing archetype that can provide services on demand at a minimal cost. The three well-known and commonly used service modelsinthecloudparadigmaresoftwareasaservice(S aaS), platform as a service (PaaS), and infrastructure as a service (IaaS).InSaaS,softwarewiththerelateddataisdeploye dbya cloud service provider, and users can use it through the web browsers. In PaaS, a service provider facilitates services to the users with a set of software programs that can solve the specific tasks. In IaaS, the cloud service provider facilitates services to the users with virtual machines and storage to improve their businesscapabilities.

Cloud computing is closely related to but not the same as grid computing [3]. Grid computing integrates diverse resourcestogetherandcontrolstheresourceswiththeun ified operating systems to provide high performance computing services, while cloud computing combines the computing and storage resources controlled by different operating sys- temstoprovideservicessuchaslarge- scaleddatastorageand high performance computing to users. The overall picture ofgridcomputinghasbeenchangedbycloudcomputin g.Distribution of data is in a new way of cloud computing comparing with the grid computing.

Cloud computing will enable services to be consumed easily on demand. Cloud computing has the characteristics such as on-demand self-

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 143-153 www.ijaem.net ISSN: 2395-5252

service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing, and transference of risk. These meritsofcloudcomputinghaveattractedsubstantialinterests from both the industrial world and the academic research world.Cloudcomputingtechnologyiscurrentlychangingthe way to do business in theworld. Cloud computing is very promising for the IT applica-

Data security has consistently been a major issue in IT. Datasecuritybecomesparticularlyseriousinthecloudcom- puting environment, because data are scattered in different machines and storage devices including servers, PCs, and variousmobiledevicessuchaswirelesssensornetworksand smart phones. Data security in the cloud computing is more complicated than data security in the traditionalinformation systems.

To make the cloud computing be adopted by users and enterprise, the security concerns of users should be rectified firsttomakecloudenvironmenttrustworthy.Thetrustworthy environment is the basic prerequisite to win confidence of users to adopt such a technology. Latif et al. discussed the assessment of cloud computing risks[7].

Beforethedatasecurityissuesarediscussed,thefunctions of cloud computing are analyzed first. Cloud computing is also known as on-demand service. In the cloud computing environment,thereisacloudserviceproviderthatfacilitates servicesandmanagestheservices.Thecloudproviderfacil- itates all the services over the Internet, while end users use services for satisfying their business needs and then pay the service provideraccordingly. Cloud computing environment provides two basic types of functions: computing and data storage. In the cloud computingenvironment,consumersofcloudservicesdonot needanythingandtheycangetaccesstotheirdataandfinish their computing tasks just through the Internet connectivity. During the access to the data and computing, the clients do notevenknowwherethedataarestoredandwhichmachines execute the computingtasks.

Coming to data storage, data protection and security are the primary factors for gaining user's trust and making the cloud technology successfully used. A number of data protectionsanddatasecuritytechniqueshavebeenproposed in the research field of cloud computing. However, data protection related techniques need to be furtherenhanced.

tions; however, there are still some problems to be solved for personal users and enterprises to store data and deploy applicationsinthecloudcomputingenvironment.One ofthe most significant barriers to adoption is data security, which is accompanied by issues including compliance, privacy, trust, and legal matters [4, 5]. The role of institutions and institutionalevolutionisclosetoprivacyandsecurityin cloud computing[6].

Services of cloud computing are provided across the entire computing spectrum. Nowadays, organizations and companies are moving and extending their business by adopting the cloud computing to lower their cost. This can contribute to free more man-powers to focus on creating strategic differentiation and business division of labor is clearer.

The cloud is growing continuously because it could provide high performance computational services at cheaper rates. Famous IT companies such as Microsoft (http://azure.microsoft.com/), Amazon(http://aws.amazon .com/), Google (https://cloud.google .com/), and Rakespace (http://www.rackspace.com/) have provided cloud service on the Internet.

The concept of cloud has a number of implementations based on the services from service providers. For example, Google Apps Engine, Microsoft Azure, and Amazon Stack are popular implementations of cloud computing provided by cloud service providers, that is, Google, Microsoft, and Amazon companies. Besides, the ACME enterprise imple- mented VMware based v-Cloud for permitting multiple organizations to share computing resources.

According to the difference of access scope, cloud can be divided into three types: public cloud, private cloud, and hybrid cloud. Public cloud is as the property of service provider and can be used in public, private cloud refers to being the property of a company, and hybrid cloud is the blendsofpublicandprivatecloud.Mostoftheexistingcloud servicesareprovidedbylargecloudservicecompaniessuch as Google, Amazon, and IBM. A private cloud is a cloud in whichonlytheauthorizeduserscanaccesstheservicesfrom the provider. In the pubic cloud anybody can use the cloud services whereas the hybrid cloud contains the concept of both public and privateclouds.

Cloud computing can save an organization's time and money, but trusting the system is more

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 143-153 www.ijaem.net ISSN: 2395-5252

important because therealassetofanyorganizationisthedatawhichtheysh are in the cloud to use the needed services by putting it either directlyintherelationaldatabaseoreventuallyinarelati onal database through anapplication.

Cloud computing brings a number of attributes that requirespecialattentionwhenitcomestotrustingthesys tem.
Thetrustoftheentiresystemdependsonthedataprotecti on and prevention techniques used in it. Numerous different tools and techniques have been tested and introduced by the researchers for data protection and prevention to gain and removethehurdleoftrustbuttherearestillgapswhichne ed attention and are required to be lined up by making these techniques much better andeffective.

Themeaningofsecurityisplentiful.Securityi sthecombi- nation of confidentiality, the prevention of the unauthorized disclosure of information, integrity, the prevention of the unauthorized amendment or deletion of information, and availability, the prevention of unauthorized withholding of information[8].

Themajorissuesinthecloudcomputinginclu deresource security, resource management, and resource monitoring. Currently, there are no standard rules and regulations to deploy applications in the cloud, and there is a lack of stan-
dardizationcontrolinthecloud.Numerousnoveltechni ques
hadbeendesignedandimplementedincloud;however,t hese techniques fall short of ensuring total security due to the dynamics of the cloud environment.

The inherent issues of data security, governance, and management with respect to control in the cloud computing are discussed in [9]. Sun et al. [10] highlighted the key security,privacy,andtrustissuesintheexistingenviron ment of cloud computing and help users to recognize the tangible and intangible threats related to its use. According to the authors, there are three major potential threats in cloud computing, namely, security, privacy, and trust. Security plays a critical role in the current era of long dreamed vision of computing as a utility. It can be divided into four subcategories:safetymechanisms,cloudservermonito ringortracing,dataconfidentiality,andavoidingmalicio usinsiders' illegal operations and servicehijacking.

Adatasecurityframeworkforcloudcomputin gnetworks is proposed [11]. The authors mainly discussed the security issues related to cloud data storage. There are also some patents about the data storage security techniques[12].YounisandKifayatgiveasurveyonsec urecloudcomputingforcriticalinfrastructure[13].Ase curityandprivacyframe- work for RFID in cloud computing was proposed for RFID technologyintegratedtothecloudcomputing[14],whi chwill
combinethecloudcomputingwiththeInternetofThing s.
In short, the foremost issues in cloud data security include data privacy, data protection, data availability, data location, and secure transmission. The security challenges in the cloud include threats, data loss, service disruption, outsidemaliciousattacks,andmultitenancyissues[15] .Chen and Zhao [16] analyzed privacy and data security issues in the cloud computing by focusing on privacy protection, datasegregation,andcloudsecurity.Datasecurityissue sare primarily at SPI (SaaS, PaaS, and IaaS) level and the major challenge in cloud computing is datasharing.

Inthispaper,wewillreviewdifferentsecurityt echniques and challenges for data storage security and privacy pro- tection in the cloud computing environment. As Figure 1 shows,thispaperpresentsacomparativeresearchanaly sisof the existing research work regarding the techniques used in the cloud computing through data security aspectsincluding data integrity, confidentiality, and availability. Data privacy issuesandtechnologiesinthecloudarealsostudied,bec ause data privacy is traditionally accompanied with datasecurity.
Comparativestudiesondatasecurityandprivacycould help to enhance the user's trust by securing data in the cloud computingenvironment.

Data integrity is easily achieved in a standalone system withasingledatabase.Dataintegrityinthestandalonesy stem
ismaintainedviadatabaseconstraintsandtransactions, which is usually finished by a database management system (DBMS). Transactions should follow ACID (atomicity, con- sistency, isolation, and durability) properties to ensure data integrity.MostdatabasessupportACIDtransactionsan

II. DATA INTEGRITY

Data integrity is one of the most critical elements in any informationsystem.Generally,dataintegritymeanspr otect- ing data from unauthorized deletion, modification, or fabri- cation. Managing entity's admittance and rights to specific enterprise resources ensures that valuable data and services are not abused, misappropriated, orstolen.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 143-153 www.ijaem.net ISSN: 2395-5252

dcan preserve dataintegrity.
Authorization is used to control the access of data. It is the mechanism by which a system determines what level of access a particular authenticated user should have to secure resources controlled by the system.
Data integrity in the cloud system means preserving informationintegrity.Thedatashouldnotbelostormodified by unauthorized users. Data integrity is the basis to provide cloud computing service such as SaaS, PaaS, and IaaS. Besides data storage of large-scaled data, cloud computing environment usually provides data processing service. Data integrity can be obtained by techniques such as RAID-like strategies and digitalsignature.

Owingtothelargequantityofentitiesandacce sspointsin acloudenvironment,authorizationiscrucialinassuring that only authorized entities can interact with data. By avoiding the unauthorized access, organizations can achieve greater confidence in data integrity. The monitoring mechanismsofferthegreatervisibilityintodeterminin gwhoorwhatmayhavealtereddataorsysteminformati on,potentiallyaffecting their integrity. Cloud computing providers are trusted to maintaindataintegrityandaccuracy.However,itisnece ssary tobuildthethirdpartysupervisionmechanismbesidesu sers and cloud serviceproviders.

Verifyingtheintegrityofdatainthecloudremo telyisthe perquisite to deploy applications. Bowers et al. proposedatheoreticalframework“ProofsofRetrievabi lity”torealizetheremotedataintegritychecking bycom biningerrorcorrection code and spot-checking [17]. The HAIL system uses POR mechanism to check the storage of data in different clouds, and it can ensure the redundancy of different copies and realizetheavailabilityandintegritychecking[18].Schi ffman et al. proposed trusted platform module (TPM) remote checkingtocheckthedataintegrityremotely[19].

III. DATA CONFIDENTIALITY

Data confidentiality is important for users to store their private or confidential data in the cloud. Authentication and access control strategies are used to ensure data confiden- tiality. The data confidentiality, authentication, and access control issues in cloud computing could be addressed by increasing the cloud reliability and trustworthiness [20].

Because the users do not trust the cloud providers and cloud storage service providers are virtually impossible to eliminate potential insider threat, it is very dangerous for users to store their sensitive data in cloud storage directly. Simpleencryptionisfacedwiththekeymanagementpr oblem and cannot support complex requirements such as query, parallel modification, and fine-grainedauthorization.

1.1. Homomorphic Encryption. Encryption is usually usedto ensure the confidentiality of data. Homomorphic encryption isakindofencryptionsystemproposedbyRivestet al.[21].
1.2. It ensures that the cipher text algebraic operation results are consistent with the clear operation after encryption results; besides,thewholeprocessdoesnotneedtodecryptt hedata. The implementation of this technique could well solve the confidentialityofdataanddataoperationsintheclo ud.

Gentry firstly proposed the fully homomorphic encryp- tion method [22], which can do any operation that can be performedincleartextwithoutdecrypting.Itisanimpor tant breakthrough in the homomorphic encryption technology. However, the encryption system involves very complicated calculation, and the cost of computing and storage is very high. This leads to the fact that the fully homomorphic encryption is still far from realapplications.

A cryptographic algorithm named Diffie-Hellman is proposed for secure communication [23], which is quite dissimilar to the key distribution management mechanism.

For more flexibility and enhanced security, a hybrid technique that combines multiple encryption algorithms such as RSA, 3DES, and random number generator has been proposed [24]. RSA is useful for establishing secure communication connection through digital signature based authentication while 3DES is particularly useful for encryp- tionofblockdata.Besides,severalencryptionalgorith msfor ensuringthesecurity ofuserdatainthecloudcomputingare discussed[25].

EncryptedSearchandDatabase.Becausethe homomor- phic encryption algorithm is inefficient, researchers turn to study the applications of limited homomorphic encryption algorithm in the cloud environment. Encrypted search is a commonoperation.
Manivannan and Sujarani [26] have proposed a light- weight mechanism for database encryption known as transposition,substitution,folding,andshifting(TSFS)algorithm.However,asthenumbersofkeysareincreas

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 143-153 www.ijaem.net ISSN: 2395-5252

ed,theamountof computations and processing alsoincreases.

In-Memory Database encryption technique is proposed for the privacy and security of sensitive data in untrusted cloud environment [27]. A synchronizer exists between the owner and the client for seeking access to the data. Client would require a key from the synchronizer to decrypt the encrypted shared data it receives from the owner. The synchronizerisutilizedtostorethecorrelatedshareddata

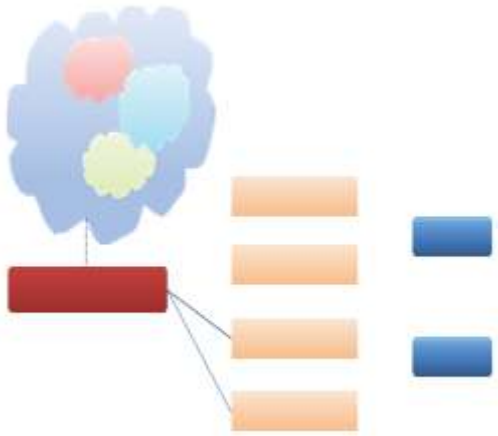

FIGURE1: Organizationofdatasecurityandprivacyincloudcomputing.

1.3. Distributive Storage. Distributive storage of data is also a promising approach in the cloud environment. AlZain et al. [30] discussed the security issues related to data privacy inthecloudcomputingincludingintegrityofdata,intrusion, and availability of service in the cloud. To ensure the data integrity,oneoptioncouldbetostoredatainmultipleclouds or cloud databases. The data to be protected from internal or external unauthorized access are divided into chunks and Shamir's secret algorithm is used to generate a polynomial functionagainsteachchunk.RamandSreenivaasan[31]have proposed a technique known as

Huang and Tso [28] proposed an asymmetric encryption mechanism for databases in the cloud. In the proposed mechanism, the commutative encryption is applied on data more than once and the order of public/private key used for encryption/decryption does not matter. Reencryption mechanismisalsousedintheproposedschemewhichshows that the cipher-text data is encrypted once again for duality. Suchschemesareveryusefulinthecloudapplicationswhere privacy is a keyconcern.

A privacy-preserving multikeyword ranked search approach over encrypted cloud data was proposed [29], which can search the encrypted cloud data and rank the search results without leakage of the user's privacy.

security as a service for securing cloud data. The proposed technique can achieve maximum security by dividing the user's data into pieces. Thesedatachunksarethenencryptedandstoredinseparated databases which follow the concept of data distribution over cloud. Because each segment of data is encrypted and separately distributed in databases over cloud, this provides enhancedsecurityagainstdifferenttypesofattacks.

Arfeenetal.[32]describethedistributionofresourcesfor cloud computing based on the tailored active measurement.Thetailoredmeasurementtechniqueisbasedonthenetworkdesignandthespecificroutesfortheincomingandoutgoingtrafficandgraduallychangingtheresourcesaccordingtotheuserneeds.Tailoredmeasurementdependsonthecomputing resources and storage resources. Because of the variable natureofnetworks,theallocationofresourcesatapartic ular time based on the tailored active method does not remain optimal. The resources may increase or decrease, so the systemhastooptimizechangesintheuserrequirementeither offlineoron-lineandtheresourceconnectivity. and the keys separately. A shortcoming of this technique is that the delays occur due to the additional communication with the central synchronizer. However, this limitation can bemitigatedbyadoptinggroupencryptionandthrough min- imizing communication between nodes andsynchronizer.

Hybrid Technique. A hybrid technique is proposed foR confidentiality and integrity [33], which uses both key sharing and authentication techniques. Theconnectivity between the user and the cloud service provider can be made more secure by utilizing powerful key sharing and authentication processes. RSA public key algorithm can be usedforsecuredistributionofthekeysbetweentheuserand cloud serviceproviders.

Athree-layereddatasecuritytechniqueisproposed[34]: thefirstlayerisusedforauthenticityofthecloudusereither by one factor or by two factor authentications; the second layer encrypts the user's data for

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 143-153 www.ijaem.net ISSN: 2395-5252

ensuring protection and privacy;andthethirdlayerdoesfastrecoveryofdatathrough a speedy decryptionprocess.

An event-based isolation of critical data in the cloud approach is proposed [35], TrustDraw, a transparentsecurity extension for the cloud which combines virtual machine introspection (VMI) and trusted computing(TC).

1.4. DataConcealment.Dataconcealmentcouldalsobeused tokeepthedataconfidentialityinthecloud.Delettreetal. [36]introducedaconcealmentconceptfordatabasessecurity. Dataconcealmentapproachesmergerealdatawiththevisualfakedatatofalsifytherealdata'svolume.However, authorized userscaneasilydifferentiateandseparatethefakedatafrom the real data. Data concealment techniques increase the overall volume of real data but provide enhanced security for the private data. The objective of data concealment is to make the real data safe and secure from malicious users and attackers. Watermarking method can serve as a key for the real data. Only the authorized users have key of watermarking, so the authentication of users is the key to ensurethetruedatatobeaccessibleforrightusers.

1.5. Deletion Confirmation. Deletion confirmation means that data could not be recovered when users delete their data after the deletion confirmation. The problem is very serious, because more than one copy exists in the cloud for the security and convenience of data recovery. When users delete their data with confirmation, all the copies of data shouldbedeletedatthesametime.However, therearesome datarecoverytechnologiesthatcouldrecoverthedatadeleted by users from the hard disks. So the cloud storage providers should ensure that the deleted data of users could not be recovered and used by other unauthenticatedusers.

To avoid the data be recovered and unauthenticatedly used, a possible approach is to encrypt the data before uploading to the cloud storage space. FADE system [37] is based on technologies such as Ephemerizer. In the system, data are encrypted before they are uploaded to the cloud storage. When users decide to delete theirdata,thesystemjusttoapplythespecificstrategytoallthestoragespacecouldbecoveredwithnewdataforreplacingthedeletionoperation.

IV. DATA AVAILABILITY

Dataavailabilitymeansthefollowing:whenaccidentssuchas hard disk damage, IDC fire, and network failures occur, the extent that user's data can be used or recovered and how the users verify their data by techniques rather than depending onthecreditguaranteebythecloudserviceprovideralone.

The issue of storing data over the transboarder servers is a serious concern of clients because the cloud vendors are governed by the local laws and, therefore, the cloud clientsshouldbecognizantofthoselaws.Moreover,the cloud serviceprovidershouldensurethedatasecurity,particularly data confidentiality and integrity. The cloud provider should share all such concerns with the client and build trust relationship in this connection. The cloud vendor should provide guarantees of data safety and explain jurisdiction of local laws to the clients. The main focus of the paper is on those data issues and challenges which are associated with datastoragelocationanditsrelocation,cost,availability,and security.

Locatingdatacanhelpuserstoincreasetheirtrustonthe cloud.Cloudstorageprovidesthetransparentstorageservice for users, which can decrease the complexity of cloud, butit also decreases the control ability on data storage of users. Bensonetal.studiedtheproofsofgeographicreplicationand succeededinlocatingthedatastoredinAmazoncloud[38].

1.6. ReliableStorageAgreement.Themostcommonabnormal behavior of untrusted storage is that the cloud service providers may discard part of the user's update data, which is hard to be checked by only depending on the simple data encryption. Additionally, a good storage agreement needs to support concurrent modification by multipleusers.

Mahajan et al. proposed Depot which can guarantee Fork-Join-Causal-Consistencyandeventualconsistency[39]. It can effectively resist attacks such as discarding and it can supporttheimplementationofothersafetyprotectionsinthe trustedcloudstorageenvironment(suchasAmazonS3).

Feldman et al. proposed SPORC [40], which can imple- ment the safe and reliable real-time interaction and collab- oration for multiple users

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 143-153 www.ijaem.net ISSN: 2395-5252

with the help of the trusted cloud environment,anduntrustedcloudserverscanonlyacce ssthe encrypteddata.
However, operation types supported by reliable storage protocolsupportarelimited,andmostofthecalculation scan only occur in theclient.

1.7. Reliability of Hard-Drive. Hard-drive is currently the main storage media in the cloud environment. Reliability of hard disks formulates the foundation of cloud storage. Pinheiro et al. studied the error rate of hard-drives based on the historical data of hard-drive [41]. They found that the error rate of hard-drives is not closely relevant to the temperature and the frequency to be used, while the error rate of hard-drives has the strong clustering characteristics.

1.8. Current SMART mechanism could not predict the error rate of hard disks. Tsai et al. studied the correlation between the soft error and hard error of hard disks, and they also found that the soft error could not predict the hard errors of hard- drives precisely [42], only about 1/3 probability that hard errors follow the soft errors.

DataPrivacy: Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal them selectively [43]. Privacy has the following ele-ments.
When: a subject may be more concerned about the current or future information being revealed than information from thepast.

How: a user may be comfortable if his/her friends can manually request his/her information, but the user may not like alerts to be sent automatically and frequently.

Extent: a user may rather have his/her information reportedasanambiguousregionratherthanaprecise point.
Incommerce,consumer'scontextandprivacyneedtobe protected and used appropriately. In organizations, privacy entails the application of laws, mechanisms, standards, and processes by which personally identifiable information is managed[44].

2. In the cloud, the privacy means when users visit the sensitivedata,thecloudservicescanpreventpotent ialadver- sary from inferring the user's behavior by the user's visit model (not direct data leakage). Researchers have focused onObliviousRAM(ORAM)technology.ORAMt echnology visits several copies of data to hide the real visiting aims of users. ORAM has been widely used in software protection and has been used in protecting the privacy in the cloud as a promising technology. Stefanov et al. proposed that apath ORAM algorithm is state-of-the-art implementation[45].

The privacy issues differ according to different cloud scenariosandcanbedividedintofoursubcategories[44, 46, 47] asfollows:

(i) how to enable users to have control over their data when the data are stored and processed in cloud and avoidtheft,nefarioususe,andunauthorizedresale,
(ii) how to guarantee data replications in a jurisdiction and consistent state, where replicating user data to multiple suitable locations is an usual choice, and avoid data loss, leakage, and unauthorizedmodifica- tion orfabrication,
(iii) whichpartyisresponsibleforensuringlegalrequir e- ments for personalinformation,
(iv) to what extent cloud subcontractors are involved in processingwhichcanbeproperlyidentified,check ed, andascertained.

5.1. Service Abuse. Service abuse means that attackers can abusethecloudserviceandacquireextradataordestroyt he interests of otherusers.
User data may be abused by other users. Deduplication technologyhasbeenwidelyusedinthecloudstorage,w hich meansthatthesamedataoftenwerestoredoncebutshare dbymultipledifferentusers.Thiswillreducethestorage spaceand cutdownthecostofcloudserviceproviders,butattacker scan accessthedatabyknowingthehashcodeofthestoredfile s.
Then,itispossibletoleakthesensitivedatainthecloud.S o proofofownershipapproachhasbeenproposedtochec kthe authentication of cloud users[48].

Attackers may lead to the cost increase of cloud service. Fraudulent resource consumption is a kind of attack on the paymentforcloudservice.Attackerscanconsumethes pecific data to increase the cost for cloud service payment. Idziorek et al. proposed this question and researched on the detection and identification of fraud resource consumption[49].

5.2. AvertingAttacks.Thecloudcomputingfacilit

ateshugeamountofsharedresourcesontheInternet.CloudsystemsshouldbecapableofavertingDenialofService(DoS)attacks.

Shen et al. analyzed requirement of security services in cloud computing [50]. The authors suggest integrating cloud services for trusted computing platform (TCP) and trusted platform support services (TSS). The trusted model should bear characteristics of confidentiality, dynamically building trust domains and dynamic of the services. Cloud infrastructures require that user transfers their data into cloudmerelybasedontrust.Neisseetal.analyzedindifferent attacks scenarios on Xen cloud platform to evaluate cloud services based on trust. Security of data and trust in cloud computingisthekeypointforitsbroaderadoption[51].

Yeluri et al. focused on the cloud services from security point of view and explored security challenges in cloud whendeployingtheservices[52].Identitymanagement,data recovery and management, security in cloud confidentiality, trust,visibility,andapplicationarchitecturearethekeypoints for ensuring security in cloudcomputing.

5.3. Identity Management. Cloud computing provides a podium to use wide range of Internet-based services [53].Butbesidesitsadvantages,italsoincreasesthesecuritythreatwhenatrustedthirdpartyisinvolved.Byinvolvingatrusted thirdparty,thereisachanceofheterogeneityofuserswhich affects security in the cloud. A possible solution to this problem could be to use a trusted third party independent approach for Identity Management to use identity data on untrustedhosts.

Squicciarini et al. focused on problems of data leakage andlossofprivacyincloudcomputing[54].Differentlevels of protections can be used to prevent data leakage and privacy loss in the cloud. Cloud computing provides new businessservicesthatarebasedondemand.Cloudnetworks have been built through dynamic virtualization of hardware, software, and datasets. Cloud security infrastructure and the trust reputation management play a vital role to upgrade the cloudservices[55].TheInternetaccesssecurity,server access security, program access security, and database security are the main security issues in the cloud.

V. CONCLUSION:

Cloud computing is a promising and emerging technology for the next generation of IT applications. The barrier and hurdlestowardtherapidgrowthofcloudcomputingare data security and privacy issues. Reducing data storage and processingcostisamandatoryrequirementofanyorganization, while analysis of data and information is always the most important tasks in all the organizations for decisionmaking. Sonoorganizationswilltransfertheirdataorinformationto the cloud until the trust is built between the cloud service providers and consumers. A number of techniques have been proposed by researchers for data protection and to attain highest level of data security in the cloud. However, there are still many gaps to be filled by making these techniquesmoreeffective.Moreworkisrequiredinthearea ofcloudcomputingtomakeitacceptablebythecloudservice consumers. This paper surveyed different techniques about data security and privacy, focusing on the data storage and use in the cloud, for data protection in the cloud computing environments to build trust between cloud service providers andconsumers.

Conflict of Interests The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments: This research work was supported by International Science and Technology Cooperation ProgramofChinaunderGrantno.2014DFA11350andtheNationalNaturalScienceFoundationofChina(Grantnos.61371185,61171014,and61202436).

REFERENCES

[1] N. Leavitt, “Is cloud computing really ready for primetime?”Computer, vol. 42, no. 1, pp. 15–25, 2009.

[2] P.MellandT.Grance,“Thenistdefinitionofcloudcomputing,” National Institute of Standards and Technology, vol. 53, no. 6, article 50,2009.

[3] F.Berman, G.Fox, and A.J.G. Hey, Grid Computing: Making the Global Infrastructurea Reality, Volume2, John Wileyandsons, 2003.

[3] M. A. Shah, R. Swaminathan, and M. Baker, “Privacy-pre- servingauditandextraction of digital contents,” IACRCryptol- ogy EPrint Archive, vol. 186,2008.

[4] Z.XiaoandY.Xiao,“Securityandprivacyincloudcomputing,” IEEE Communications Surveys &Tutorials, vol. 15, no. 2, pp. 843–859,2013.

[5] N.Kshetri,“Privacyandsecurityissuesincloud

computing:theroleofinstitutionsandinstitutionalevolution,"Telecommunica-tionsPolicy,vol.37,no.4-5,pp.372–386,2013.

[6] R.Latif,H.Abbas,S.Assar,andQ.Ali,"Cloudcomputingrisk assessment: a systematic literature review," in Future Informa-tionTechnology,pp.285–295,Springer,Berlin,Germany,2014.

[7] A.Avižienis,J.Laprie,B.Randell,andC.Landwehr,"Basic concepts and taxonomy of dependable and secure computing," IEEETransactionsonDependableandSecureComputing,vol.1, no. 1, pp. 11–33,2004.

[8] Z. Mahmood, "Data location and security issues in cloud computing," in Proceedings of the 2nd International Conference on Emerging Intelligent Dataand Web Technologies (EIDWT'11), pp. 49–54, IEEE, September 2011.

[9] D. Sun, G. Chang, L. Sun, and X. Wang, "Surveying and ana- lyzing security, privacy and trust issues in cloud computing environments,"inProceedingsoftheInternationalConferenceon Advancedin Control Engineering and InformationScience(CEIS'11),pp.2852–2856,chn,August2011.

[10] A. Pandey, R. M. Tugnayat, and A. K. Tiwari, "Data Security Framework for Cloud Computing Networks," International JournalofComputerEngineering&Technology,vol.4,no.1,pp. 178–181,2013.

[11] D.A.Klein,"Datasecurityfordigitaldatastorage,"U.S.Patent Application 14/022,095,2013.

[12] M. Y. A. Younis and K. Kifayat, "Secure cloud computing for critical infrastructure: a survey," Tech. Rep., Liverpool John Moores University, Liverpool, UK,2013.

[13] S.Kardaş,S.Çelik,M.A.Bingöl,andA.Levi,"Anewsecurity and privacy framework for RFID in cloud computing," in Proceedingsofthe5thIEEEInternationalConferenceonCloud Computing Technology and Science (Cloud Com'13), Bristol,UK, 2013.

[14] A. Behl, "Emerging security challenges in cloud computing: an insight to cloud security challenges and their mitigation," in Proceedings of the World Congress on Information and Communication Technologies (WICT '11), pp. 217–222, IEEE, December2011.

[15] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," in Proceeding of the International Conference on Computer Science and Electronics Engineering (ICCSEE'12),vol.1,pp.647–651, Hangzhou,China,March2012.

[16] K. D. Bowers, A. Juels, and A. Oprea, "Proofs of retrievabil- ity: theory and implementation," in Proceedings of the ACM Workshopon CloudComputingSecurity(CCSW'09),pp.43–53, November2009.

[17] K.D.Bowers,A.Juels,andA.Oprea,"HAIL:ahighavailabilityandintegritylayerforcloudstorage,"inProceedingsofthe16thACMconferenceonComputerandCommunicationsSecurity,pp.187-198, ACM, Chicago, Ill, USA, November2009.

[18] J. Schiffman, T. Moyer, H. Vijayakumar, T. Jaeger, and P. McDaniel," Seedingclouds with trustanchors," in Proceedings of the ACM workshop on Cloud computing security workshop (CCSW'10),pp.43–46,ACM,October2010.

[19] D. H. Rakesh, R. R. Bhavsar, and A. S. Thorve, "Data security overcloud," International Journal of Computer Applications,no. 5, pp. 11–14,2012.

[20] R.L.Rivest,L.Adleman,andM.L.Dertouzos," Ondatabanks and privacy homomorphisms," Foundations of Secure Computation,vol.4,no.11,pp.169–180,1978.

[21] C. Gentry, A fully homomorphic encryption scheme [Ph.D. thesis], Stanford University,2009.

[22] D.Boneh,"Thedecision Diffie-Hellmanproblem,"inAlgorith- mic Number Theory, vol. 1423,pp.48–63, Springer,1998.

[23] A. Kaur and M. Bhardwaj, "Hybrid encryption for cloud databasesecurity," Journal of Engineering Science Technology, vol. 2, pp. 737–741,2012.

[24] R. Arora, A. Parashar, and C. C. I. Transforming, "Secureuser dataincloud computing using encryption algorithms," International JournalofEngineeringResearchandApplications,vol.3, no. 4, pp. 1922–1926,2013.

[25] D. Manivannan and R. Sujarani, "Light weight and secure database encryption using tsfs algorithm," in Proceedings of theInternationalConferenceonComputingCommunicationand NetworkingTechnologies(ICCCNT'10),pp.1–7,IEEE,2010.

[26] F. Pagano and D. Pagano, "Using in-memory encrypted databaseson the cloud," in Proceedings of the1stIEEEInternationalWorkshoponSecuringServicesontheCloud(IWSSC'11), pp. 30–37, September2011.

[27] K.HuangandR.Tso,"Acommutativeencryptio

nschemebased on ElG amal encryption," in Proceedings of the 3rd International Conferenceon Information Security and Intelligent Control (ISIC'12), pp.156–159,IEEE,August2012.

[28] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-pre- serving multi-keyword ranked search over encrypted cloud data,"IEEETransactionsonParallelandDistributedSystems,vol. 25, no. 1, pp. 222–233,2014.

[29] M. A. AlZain, B. Soh, and E. Pardede, "Mcdb: using multi- clouds to ensure security in cloud computing," in Proceedings oftheIEEE9thInternationalConferenceonDependable,Auto-nomicandSecureComputing(DASC'11),pp.784–791,2011.

[30] C. P. Ram and G. Sreenivaasan, "Security as a service (sass): securing user data by coprocessor and distributing the data,"in Proceedings of the 2nd International Conference on Trendz inInformationSciencesandComputing,(TISC'10),pp.152–155, IEEE, December2010.

[31] M.AsadArfeen,K.Pawlikowski,andA.Willig, "Aframework for resource allocation strategies in cloud computing environment," in Proceedings of the 35th Annual IEEE International Computer Software and Applications Conference Workshops (COMPSACW'11),pp.261–266,July2011

[32] A. Rao, "Centralized database security in cloud," International JournalofAdvancedResearchinComputerand Communication Engineering,vol.1,pp.544–549,2012.

[33] E.M.Mohamed,H.S.Abdelkader,andS.ElEtriby,"Enhanceddatasecuritymodelforcloudcomputing,"inProceedingsofthe 8thInternationalConferenceonInformaticsand Systems(INFOS '12), pp. CC-12–CC-17, IEEE,2012.

[34] S. Biedermann and S. Katzenbeisser, "POSTER: event-based isolation of criticaldatain the cloud,"inProceedingsoftheACMSIGSACConferenceonComputer&CommunicationsSecurity, pp. 1383–1386, ACM,2013.

[35] C. Delettre, K. Boudaoud, and M. Riveill, "Cloud computing, securityanddataconcealment,"inProceedingsofthe16thIEEESymposiumonComputersandCommunications(ISCC'11),pp. 424–431, Kerkyra, Greece, July2011.

[36] Y. Tang,P.P.C.Lee,J.C.S.Lui,andR.Perlman,"Fade:secure overlay cloud storage with file assured deletion," in Security andPrivacyinCommunicationNetworks,pp.380–397,Springer, New York, NY, USA,2010.

[37] K.Benson,R.Dowsley,andH.Shacham,"Doyouknowwhere yourcloudfilesare?" inProceedingsofthe3rdACMworkshopon Cloudcomputingsecurityworkshop,pp.73–82,ACM,October 2011.

[38] P. Mahajan, S. Setty, S. Lee et al., "Depot: cloud storage with minimaltrust,"ACMTransactionsonComputer Systems,vol.29, no. 4, article 12,2011.

[39] A. J. Feldman, W. P. Zeller, M. J. Freedman, and E. W. Felten, "SPORC: groupcollaboration using untrusted cloud resources," in Proceedings of the 9th USENIX Conference on Operating SystemsDesignandImplementation(OSDI'10),vol.10,pp.337– 350,2010.

[40] E.Pinheiro,W.D.Weber,andL.A.Barroso,"Failuretrendsinalargediskdrivepopulation,"inProceedingsofthe5thUSENIX conferenceonFileandStorageTechnologies(FAST'07),vol.7,pp. 17–23.

[41] T.Tsai,N.Theera-Ampornpunt,andS.Bagchi,"Astudyofsoft error consequences in hard disk drives," in Proceeding of the 42nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks(DSN'12),pp.1–8,Boston,Mass,USA, June2012.

[42] J. Krumm, "A survey of computational location privacy," Per- sonal and Ubiquitous Computing, vol. 13, no. 6, pp. 391–399, 2009.

[43] S.PearsonandA.Benameur,"Privacy,securityandtrustissuesarisingfromcloudcomputing,"in Proceedingsofthe2ndIEEE International Conference on Cloud Computing Technologyand Science(CloudCom'10),pp.693–702,IEEE,December2010.

[44] E.Stefanov,M.vanDijk,E.Shietal.,"Pathoram: anextremely simple oblivious ram protocol," in Proceedings of the ACM SIGSACConferenceonComputer&CommunicationsSecurity, pp. 299–310, ACM,2013.

[45] S. Paquette, P. T. Jaeger, and S. C. Wilson, "Identifying the security risks associated with governmental use of cloud computing," Government Information Quarterly, vol. 27, no. 3, pp. 245–253,2010.

[46] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud," Journal of Network and

ComputerApplications,vol.34,no.1,pp.1–11,2011.

[47] C. Cachin and M. Schunter, "A cloud you can trust," IEEE Spectrum,vol.48,no.12,pp.28–51,2011.

[48] J. Idziorek, M. Tannian, and D. Jacobson, "Attribution of FraudulentResource Consumptionin the cloud,"inProceedings of the IEEE 5th International Conference on CloudComputing (CLOUD'12),pp.99–106,June2012.

[49] Z. Shen, L. Li, F. Yan, and X. Wu, "Cloud computing system based on trusted computing platform," in Proceedings of the InternationalConferenceonIntelligentComputationTechnology andAutomation (ICICTA'10), vol.1, pp. 942–945,IEEE,May 2010.

[50] R. Neisse, D. Holling, and A. Pretschner, "Implementing trust incloud in frastructures," inProceedingsofthe11thIEEE/ACM International SymposiumonCluster,CloudandGridComputing (CCGrid'11), pp.524–533, IEEE ComputerSociety,May2011.

[51] R. Yeluri, E. Castro-Leon, R. R. Harmon, and J. Greene, "Building trust and compliance in the cloud for services," in ProceedingsoftheAnnualSRIIGlobalConference(SRII'12),pp. 379–390,San Jose, Calif, USA, July 2012.

[52] R. Ranchal, B. Bhargava, L. B. Othmane et al., "Protection of identity information in cloud computing without trusted third party,"inProceedingsofthe29thIEEESymposiumonReliable DistributedSystems (SRDS'10), pp.368–372,November2010. A. Squicciarini, S. Sundareswaran, and D. Lin, "Preventing information leakagefromindexinginthecloud,"inProceedings of the 3rd IEEE International Conference on Cloud Computing (CLOUD'10),pp.188–195,July2010.

[53] K. Hwang and D. Li, "Trusted cloud computing with secure resourcesanddata coloring," IEEEInternetComputing,vol.14, no. 5, pp. 14–22,2010.

International Journal of Advances in Engineering and Management
ISSN: 2395-5252

IJAEM

Volume: 03 Issue: 03 DOI: 10.35629/5252

www.ijaem.net
Email id: ijaem.paper@gmail.com