International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X;pISSN:2321-2241 Volume: 5; Issue: 3; March -2016

Cloud Computing Security for User Data

D. B.Rathod [1], Dr.G.Mahadevan [2], Poornaprazna.M.G [3],

[1,3]SRN Adarsh College,Bangalore,India

[2] Annai College of Engineering and Technology, Tamilnadu, India

Abstract : It is well-known that cloud computing has many potential advantages and many enterprise applications and data are migrating to public or hybrid cloud. A general understanding of cloud computing refers to the following concepts: grid computing, utility computing, software as a service, storage in the cloud and virtualization. From the consumers' perspective, cloud computing security concerns, especially data security and privacy protection issues, remain the primary inhibitor for adoption of cloud computing services. This paper provides a concise but all-round analysis on data security and privacy protection issues associated with cloud computing across all stages of data life cycle. Then this paper discusses some current solutions. Finally, this paper describes future research work about data security and privacy protectionissues in cloud. The typical systems that require privacy protection are e-commerce systems that store credit cards and health care systems with health data. The ability to control what information to reveal and who can access that information over the internet has become a security concern. These concerns include whether personal informationcan be stored or read by third parties without consent, or whether third parties can track the web sites someone has visited. Another concern is whether web sites which are visited collect, store, and possibly share personal information about users. The key to privacy protection in the cloud environmentis the strict separation of sensitive data from non-sensitive data followed by the encryption of sensitive elements.

Keywords- cloud computing, virtualization, access control,grid computing,utility computing,virtualization cloud computing,security,data segregation, data security, privacy protection.

Introduction:

Cloud computing is defined as management and provision of resources, software, applications and information as services over the cloud (internet) on demand. Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. With its ability to provide users dynamically scalable, shared resources over the internet cloud computing has emerged as a promising hosting platform that performs an intelligent usage of a collection of services, applications, information and infrastructure comprised of pools of computer, network, information and storage resources. Cloud Computing uses internet and central remote servers to maintain data and applications.

Although cloud service providers can offer benefits to users, security risks play a major role in the cloud computing environment. Users of online data sharing or network facilities are aware of the potential loss of privacy. Protecting private and important information such as credit card details or patients' medical records from attackers or malicious insiders is of critical importance. However storing a large amount of data including critical information on the cloud motivates highly skilled hackers to hack the data.Thus creating a need for the security to be considered as one of the top issues while considering Cloud Computing.

There are three service models and four deployment models. The threeservice models are: Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS) and CloudInfrastructure as a Service (IaaS). The four deployment modelsare: Private cloud, Community cloud, Public cloud and Hybridcloud. Compared with the traditional IT model, the cloudcomputing has many

potential advantages. But from theconsumers' perspective, cloud computing security concernsremain a major barrier for the adoption of cloud computing.The primary reason not to use cloud computing services is that there are data security and privacy concerns.Security vulnerabilities in Google Docs lead to serious leakage of user private information. Google Gmail also appeared a global failure up to 4 hours. People with ulterior motives can take advantage of the vulnerability in the Windows virtual machine on the host Mac to executemalicious code. Serious security incidents even lead to collapse of cloud computing vendors. As administrators' misuse leading to lossof 45% user data, cloud storage vendor LinkUp had beenforced to close.Security control measures in cloud are similar to ones intraditional IT environment. Cloudcomputing may face different risks and challenges and also traditional security issues are still present in cloudcomputing environments.

Due to theopenness and multi-tenant characteristic of the cloud, cloudcomputing is bringing tremendous impact on informationsecurity field:

(1) Due to dynamic scalability, service abstraction, andlocation transparency features of cloud computing models, allkinds of applications and data on the cloud platform have nofixed infrastructure and security boundaries. In the event ofsecurity breach, it's difficult to isolate a particular physicalresource that has a threat or has been compromised.

(2) According to the service delivery models of cloudcomputing, resources cloud services based on may be ownedby multiple providers. As there is a conflict of interest, it isdifficult to deploy a unified security measures;

(3) As the openness of cloud and sharing virtualizedresources by multi-tenant, user data may be accessed by otherunauthorized users.

(4) As the cloud platform has to deal with massiveinformation storage and to deliver a fast access, cloud securitymeasures have to meet the need of massive information processing.

This paper describes data security and privacy protectionissues in cloud. This paper is organized as follows: Section I gives a brief description of what exactly cloud computing security-related issues are. Section II discusses data securityand privacy protection issues associated with cloud computingacross all stages of data life cycle. Section III shows current solutions for data security and privacy protection issues incloud. Section IV summarizes the contents of this paper. SectionV describes future research work.

I. Cloud Computing Security Issues

A. Cloud Computing Security

Wikipedia[1] defines Cloud Computing Security as "*Cloudcomputing security (sometimes referred to simply as "cloud security") is an evolving sub-domain of computer security,network security, and, more broadly, information security. Itrefers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.*" Note that cloud computingsecurity referred to here is not cloud-based security softwareproducts such as cloud-based anti-virus, anti-spam, and so on.

B. Security Issues Associated with the Cloud

There are many security issues associated with cloud computing and they can be grouped into any number ofdimensions. According to Gartner[2], before making a choice of cloudvendors, users should ask the vendors for seven specific safety issues: Privileged user access, regulatory

compliance, datalocation, data segregation, recovery, investigative support and long-term viability. In 2009, Forrester Research Inc.[3], evaluated security and privacy practices of some of the leadingcloud providers (such as Salesforce.com, Amazon, Google, andMicrosoft) in three major aspects: Security and privacy,

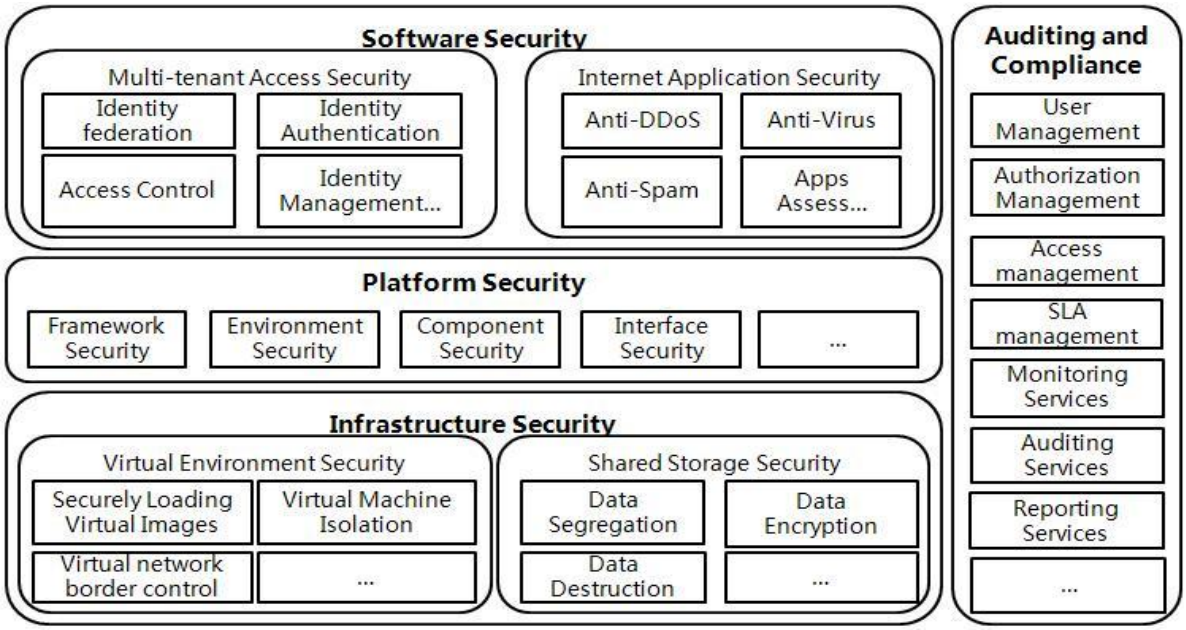

Figure-1: Cloud computing security architecture

compliance, and legal and contractual issues. Cloud SecurityAlliance (CSA) [4] is gathering solution providers, non-profitsand individuals to enter into discussion about the current andfuture best practices for information assurance in the cloud.The CSA has identified thirteen domains of concerns on cloudcomputing security[5].S. Subashini and V. Kavitha made an investigation of cloudcomputing security issues from the cloud computing servicedelivery models (SPI model) and give a detailed analysis andassessment method description for each security issue[6].Mohamed Al Morsy, John Grundy and Ingo Müller exploredthe cloud computing security issues from different perspectives,including security issues associated with cloud computingarchitecture, service delivery models, cloud characteristics andcloud stakeholders[7]. Yanpei Chen, Vern Paxson and RandyH. Katz believed that two aspects are to some degree new andessential to cloud: the complexities of multi-party trustconsiderations, and the ensuing need for mutual auditability.

They also point out some new opportunities in cloudcomputing security[8].According to the SPI service delivery models, deploymentmodels and essential characteristics of cloud, there are securityissues in all aspects of the infrastructure including networklevel, host level and application level.

II. Data security And Privacy Protection Issues

The content of data security and privacy protection in cloudis similar to that of traditional data security and privacyprotection. It is also involved in every stage of the data lifecycle. But because of openness and multi-tenant characteristicof the cloud, the content of data security and privacy protectionin cloud has its particularities.The concept of privacy is very different in different

countries, cultures or jurisdictions. The definition adopted byOrganization for Economic Cooperation and Development (OECD) [9] is "*any information relating to an identified or identifiable individual (data subject).*" Another populardefinition provided by the American Institute of CertifiedPublic Accountants (AICPA) and the Canadian Institute ofChartered Accountants (CICA) in the Generally AcceptedPrivacy Principles (GAPP) standard is "*The rights andobligations of individuals and organizations with respect to thecollection, use, retention, and disclosure of personalinformation" P*rivacy is associated withthe collection, use, disclosure, storage, and destruction of personal data (or personally identifiable information, PII). Identification of private information depends on the specificapplication scenario and the law, and is the primary task of privacy protection.

II. Current Security Solutions For Data Security

IBM developed a fully homomorphic encryption scheme inJune 2009. This scheme allows data to be processed withoutbeing decrypted [10]. Roy I and Ramadan HE applieddecentralized information flow control (DIFC) and differentialprivacy protection technology into data generation andcalculation stages in cloud and put forth a privacy protection system called airavat [11]. This system can prevent privacyleakage without authorization in Map-Reduce computingprocess. A key problem for data encryption solutions is keymanagement. On the one hand, the users have not enoughexpertise to manage their keys. On the other hand, the cloudservice providers need to maintain a large number of user keys.The Organization for the Advancement of Structured Information Standards (OASIS) Key ManagementInteroperability Protocol (KMIP) is trying to solve such issues[12].About data integrity verification, because of datacommunication, transfer fees and time cost, the users can notfirst download data to verify its correctness and then upload thedata. And as the data is dynamic in cloud storage, traditionaldata integrity solutions are no longer suitable. NEC Labs'sprovable data integrity (PDI) solution can support public data integrity verification [13]. Cong Wang proposed amathematical way to verify the integrity of the datadynamically stored in the cloud [14].In the data storage and use stages, Mowbray proposed a client-based privacy management tool [15]. It provides a usercentrictrust model to help users to control the storage and useof their sensitive information in the cloud. Munts-Mulerodiscussed the problems that existing privacy protectiontechnologies (such as K anonymous, Graph Anonymization,and data pre-processing methods) faced when applied to largedata and analyzed current solutions [16]. The challenge of dataprivacy is sharing data while protecting personal privacyinformation. RandikeGajanayake proposed a privacyprotection framework based on information accountability (IA)components [17]. The IA agent can identify the users who are accessing information and the types of information they use.When inappropriate misuse is detected, the agent defines a setof methods to hold the users accountable for misuse.About data destruction, U.S. Department of Defense (DoD)shows two approved methods of data(destruction) security, but it does not provide any specificrequirements for how

these two methods are to be achieved[18]. The National Institute of Standards and Technology(NIST) Special Publication [19].givesa"*Guidelinesfor Media Sanitization.*"

IV. Conclusion

Although cloud computing has many advantages, there arestill many actual problems that need to be solved. According toa Gartner survey about cloud computing revenues, market sizefor Public and Hybrid cloud is $59 billion and it will reachUSD 149B by 2014 with a compound annual growth rate of20[22]. The revenue estimation implies that cloud computing isa promising industry. But from another perspective, existingvulnerabilities in the cloud model will increase the threats from hackers.According to service delivery models, deployment modelsand essential features of the cloud computing, data security andprivacy protection issues are the primary problems that need tobe solved as soon as possible. Data security and privacy issues exist in all levels in SPI service delivery models and in allstages of data life cycle.The challenges in privacy protection are sharing data whileprotecting personal information. The typical systems thatrequire privacy protection are e-commerce systems that storecredit cards and health care systems with health data. Theability to control what information to reveal and who canaccess that information over the Internet has become a growingconcern. These concerns include whether personal informationcan be stored or read by third parties without consent, orwhether third parties can track the web sites someone hasvisited. Another concern is whether web sites which are visited collect, store, and possibly share personal information aboutusers. The key to privacy protection in the cloud environmentis the strict separation of sensitive data from non-sensitive datafollowed by the encryption of sensitive elements.According to the analysis for data security and privacy protection issues above, it is expected to have an integrated andcomprehensive security solution to meet the needs of defensein depth. Regarding privacy protection, privacy dataidentification and isolation are the primary tasks. They shouldbe considered during the design of cloud-based applications.

V. Future Work

For data security and privacy protection issues, thefundamental challenges are separation of sensitive data andaccess control. Our objective is to design a set of unifiedidentity management and privacy protection frameworks acrossapplications or cloud computing services. As mobility of employees in organizations is relatively large, identitymanagement system should achieve more automatic and fastuser account provisioning and de-provisioning in order toensure no un-authorized access to organizations' cloudresources by some employees who has left the organizations.Authorization and access control mechanisms should achieve aunified, reusable and scalable access control model and meetthe need of fine-grained access authorization. Accountabilitybased privacy protection mechanisms will achieve dynamicaland real-time inform, authorization and auditing for the dataowners when their private data being accessed.

VI. References:

[1] Cloud computing security, http://en.wikipedia.org/wiki/Cloud_computing_security.
[2] Gartner: Seven cloud-computing security risks. InfoWorld.2008-07-02.
http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputing-security-risks-853.
[3] Cloud Security Front and Center. Forrester Research. 2009-11-18.
http://blogs.forrester.com/srm/2009/11/cloud-security-front-andcenter.html

[4] Cloud Security Alliance. http://www.cloudsecurityalliance.org.
[5] Cloud Security Alliance, Security Guidance for Critical Areas of Focusin Cloud Computing,
[6] S. Subashini, V.Kavitha. A survey on security issues in service deliverymodels of cloud computing. Journal of Network and ComputerApplications 34(2011)1-11.
[7] Mohamed Al Morsy, Ingo Müller, "An Analysis of TheCloud Computing Security Problem," in Proceedings of APSEC 2010Cloud Workshop, Sydney, Australia, 30th Nov 2010.
[8] Yanpei Chen, Vern Paxson, Randy H. Katz, "What's New About CloudComputing Security?" Technical Report No.UCB/EECS-2010-5.http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html
[9] "OECD Guidelines on the Protection of Privacy and Transborder Flowsof Personal Data," http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.
[10] "IBM Discovers Encryption Scheme That Could Improve Cloud Security, Spam Filtering," at http://www.eweek.com/c/a/Security/IBMUncovers-Encryption-Scheme-That-Could-Improve-Cloud-Security-Spam-Filtering-135413/.
[11] Roy I, Ramadan HE, Setty STV, Kilzer A, Shmatikov V, Witchel E."Airavat: Security and privacy for MapReduce," In: Castro M, eds. Proc.of the 7th UsenixSymp. on Networked Systems Design andImplementation. San Jose: USENIX Association, 2010. 297.312.
[12] "OASIS Key Management Interoperability Protocol (KMIP) TC", http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip.
[13] Zeng K, "Publicly verifiable remote data integrity," In: Chen LQ, RyanMD, Wang GL, eds. LNCS 5308. Birmingham: Springer-Verlag, 2008.419.434.
[14] Cong W,Qian Wang, KuiRen, and Wenjing Lou, "Ensuring DataStorage Security in loud Computing,"in Proceedings of the 17th International Workshop on Quality of ervice.2009:1-9.
[15] Bowers KD, Juels A, Oprea A. Proofs of retrievability: Theory andimplementation. In: Sion R, ed. Proc. of the 2009 ACM Workshop onCloud Computing Security, CCSW 2009, Co-Located with the 16th ACM Computer and Communications Security Conf., CCS 2009. NewYork: Association for Computing Machinery, 2009. 43.54. [doi:10.1145/1655008.1655015]