International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 06, June-2015

Data Security in Public Cloud Storage Environment

Dr. Ramalingam Sugumar
Professor,
Christhuraj Institute of Computer Application
Panjappur, Trichy-12.

Sharmila Banu Sheik Imam
Lecturer, Dept. of CCSIT,
King Faisal University,
Al-Hassa, KSA.

***Abstract* – Cloudcomputing is an internet based computing. It is evolved from grid computing, utility computing, parallel computing, distributed computing and virtualization. It has more powerful computing infrastructure with a pool of thousands of computers and servers. Cloud helps the Small and Medium scale Enterprises (SME) with lots of virtual storage spaces. Enterprises are interested to outsource their data to cloud but due to some security issues most of the enterprises reluctant to adopt the cloud. Security is the most importance concern in cloud computing. Securing the outsourced data in the cloud storage is most important for the cloud providers and users. This paper describes about the characteristics, issues and importance of security in public cloud environment. Data outsourcing creates many security challenges to both cloud providers and users. By address this challenges, the users are adopted the cloud without any hesitation.**

***Keywords* : Cloud Computing; Cloud Users; Cloud Providers; Security; Outsourcing;**

I. INTRODUCTION

Nowadays, Cloud Computing is the hottest topic in information technology(IT). However, it is not so much that the term 'Cloud Computing' representsa host of new technologies, but rather that these technologies are combinedand effectively upgraded and enable new IT services and newbusiness models [1].The major feature of cloud computing is that it allows sharing and scalable deployment of services as needed by the users from any location. Cloud computing saves time and money during software up-gradation; cloud services are updated by the provider; so users are always working on the latest platform [2]. Cloud minimizes the amount of wasted computing resources and can also reduce energy consumption significantly.

The main core area of Cloud computing is Virtualization [3]. Virtualization empowers the cloud as a scalable and elastic service environment[4]. It enables a dynamic datacentre where servers provide a pool of resources that are connected as needed, where the relationship of applications to compute, storage, and network resources changes dynamically in order to meet both workload and business demands.

Cloud computing incorporateseventslike use of social networking sites and other methods of interactive computing; however, cloud computing is always concerned with gain access to online software applications, data storage[5]. Cloud computing increases the capacity or add capabilities dynamically without any investment in new infrastructure, training new personnel, or licensing new software. It extends Information Technology's (IT) existing capabilities[6] to unlimited provisioning. Recently, cloud computing grows from being anauspicious business method to small and medium scale enterprises. But as more and more dataof users are stored in the cloud storage, worries areraised about how to protectthe cloud environment. In spite ofof all the publicity surrounding the cloud, customers are still unwilling to outsource their business in the cloud. Security problems in cloud has played a major role in slowing down its acceptance, in fact security is ranked at first in the survey of ICT on 2009 as depicted in Figure 1.

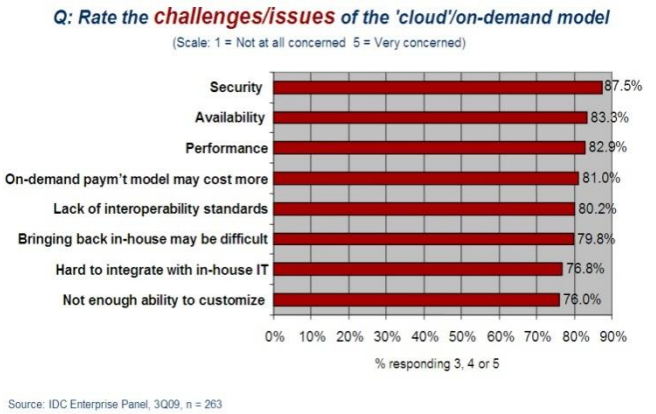

Figure 1. IDC IT Cloud Services Survey [7]

Cloud computing with many new technologies and services, information security and data protection issues are intensely debated and examined. Many surveys and studies reveal that potential cloud users have concerns about information security and data protection which stand in the way of a wider deployment. The required trust still needs to be developed for secure cloud environment. It is defined by NIST [8], cloud has five essential characteristics, three services and four deployment models.

II. RELATED WORKS

Cloud computing brings out with extensive service benefits including service flexibility, configurable computing resources, Reliability and economic savings [9]. Though, security concerns are the primary challengeswhen adoptingthe cloud to the users [10]. The concepts that cloud presents, such asresource sharing,multi-tenancy and outsourcing, produce new challenges to the cloud data

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

storage security. To address these challenges, it is necessary to enhance the security mechanism developed for traditional computing systems and proposing a new security policies, models and protocols [11] for cloud.

Khalil et al., [12] provides a comprehensive study of cloud computing security concerns and identify cloud vulnerabilities. Vulnerabilities are classified into security threats and attacks. It is important to neutralize the threats, control the vulnerabilities and calibrate the attacks in public cloud environment.

Gartner [13] recognizedsome security problems that must be clarified with cloud providers before adopting the cloud computing model. That are,*(i) Privileged user access,(ii) Regulatory compliance,(iii) Data location,(iv) Data segregation, (v) Recovery,(iv) Investigative support*, (vii) *Long-term viability*.ENISA examined the several security risksrelated to adopting cloud computing along with the affected assets, the risks likelihood, impacts,and vulnerabilities in the cloud computing may lead to such risks[14]. The Cloud Computing Use CaseDiscussion Group reviews the different scenarios and related requirements that may exist in the cloud model. They consider use cases from different perspectives includingcustomers, developers and security engineers[15].

Berndet al, [16] discussed the security challenges existing in the cloud platform. The authors groupedthe possible challengesinto cloud characteristics-related, security related. Kresimir et al, [17]focused on high level security problems in the cloudcomputing model such as data integrity, payment and privacy of sensitive information. Balachandra et al, [18] described the service level agreements specification and objectives related to data locations, segregationand data recovery.

Subashini et al,[19]discussed the security concerns in different cloud service model,they are focusing on the SaaS model.Morsy et al, [20]inspected cloud computingproblems from the cloud architecture, cloud characteristics, cloud stakeholders, and cloudservice models perspectives.Ragovind et al, [21] discussed the management of security inCloud computing focusing on Gartner's list on cloud security issues and the findings from theInternational Data Corporation enterprise.

A recent survey by Cloud Security Alliance(CSA) [22] shows that SMEs are eager to adopt cloud computing butthat security isdesired both to accelerate cloud adoption on a wide scale and to respond toregulatory drivers. It also details that cloud computing are shaping the future of IT but the absenceof a compliance environment is having dramatic impact on cloud computing growth.

Severalstudies have been carried out relating to security issues in cloud computing but this paperpresents a detailed analysis of the cloud computing security issues and challenges and importance of security in cloud computing.

III. Issues in Cloud Data Storage

Cloud Computing moves the application and data to thecloud storage, where the management of the data and services may not be fully trustworthy. This uniqueattribute, however, poses many new security challengeswhich have not been well understood[23]. This paper focuseson cloud data storage security, which has always been animportant aspect of quality of service. Following are theissues [24] in cloud data storage.

A. Privacy

Cloud computing utilizes the virtual computing technology unlike traditional computing model.Users' personal data are scattered in different clouddata center rather than stored in the single physical location,even across the national borders. At this time, data privacyprotection faces the disagreement of different legalsystems. Moreover, users may losetheir hiddeninformation when they are accessing cloud computingservices. Attackers could analyze the critical task dependingon the computing task submitted by the users.The major privacy issues [25] are i) Trust, ii) Uncertainty and iii) Compliance.

B. Security

Security problems are related to areas such as external datastorage, dependency on the public internet, lack of control,multi-tenancy and integration with internal security [26].Cloud providers employ data storage andtransmission, encryption, user authentication, andauthorization. Many clients concern on the vulnerability ofremote data to hackers.

C. Trust

Trust issue in cloud computing has equal concern againstsecurity and privacy. Trust is defined as reliance on the integrity, strength, ability and surety of a person or thing.Entrusting user data on to a third party who is providing cloud services is an issue. For example, in April 2012,Amazon's Elastic Compute Cloud service crashed during a system upgrade, knocking customers' websites off-line allover for several hours for several days. Another incident happened on the same month. The hackers broke into theSony PlayStation Network, exposing the personalinformation to 77 million people around the world. Theseissues have certainly created doubts in mind of cloud usersand damaged the trust [24].

D. Ownership

Once data has been submitted to the cloud, developershave concern about losing their rights or being unable toprotect the rights of their customers. Many cloud providersaddress this issue with well-skilled user-sided agreements.According to the agreement, users would be wise to seek advice from their favourite legal representative.

E. Performance and Availability

Business organizations are worried about acceptable levelsof performance and availability of applications hosted inthe cloud. Application and data in the cloud storage shouldbe available to the users at anytime and anywhere. Users have no worry about the local system which is used foraccessing the cloud servers.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

F. *Long-term Viability*

Users should be sure that the data put into the cloud willnever become invalid even the cloud computing providerget lost or get acquired and swallowed up by a largercompany. Users should ask their potential providers of cloud how they would get user's data back and if it wouldbe in a format that user could import into a replacementapplication [27].

H. Data Backup

Cloud providers employ redundant servers and routinedata backup processes, but users worry about being able tocontrol their own backups. Many providers are nowoffering data dumps onto media or allowing users to backup data through regular downloads.

G. Data Portability and Conversion

Users have concerns on data portability like, switchingbetween service providers. There may be difficulty intransferring data. Porting and converting data is highly dependent on the nature of the cloud provider's dataretrieval format, particularly in cases where the formatcannot be easily revealed. As service competition grows,open standards become established, the data portabilityissue will ease, and conversion processes will becomeavailable supporting the more popular cloud providers.Worst case is that the cloud subscribers have to pay forsome custom data conversion.

These are certain areas in which cloud computing requiresto excel and solve problem related to it. Out of all the problems; narrated Security and Privacy [28] put the majorthreats in growth of cloud computing. It needs to be worked upon.

IV. Cloud Data Outsourcing

The new concept introduced by the cloud is data outsourcing. Data outsourcing in the public cloud is becoming increasingly popular and introducing a new paradigm, called Database as a Service, where users' data are stored at an external CSP [29]. This scenario presents new research challenges on which the usability of the system is based [30].

The main advantage of outsourcing is related to the cost of on-premises versus outsourced hosting; outsourcing provides,

- Significant cost savings and service benefits and
- Higher availability and more effective disaster protection than on-premises operation.

Users could outsource data to cloud and retrieve the same when they are needed. Cloud service providers should store the users' data in the database server and provide maximum availability of data and efficient disaster recovery. The data outsourcing scenario in public cloud is represented in Figure 2and Figure 3. Cloud users may be the enterprise users or general users [31].

Outsourced data could be accessed in following two schemes. In the first scheme, data owners and data users are same, where as in the second scheme, data owners and data users are different. Figure 2 represents the first scheme and Figure 3 represents the second scheme.

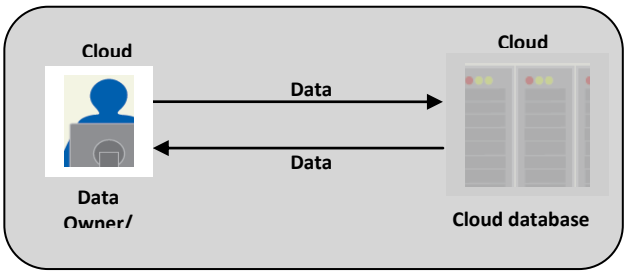

Figure 2. Data Outsourcing in Public Cloud Storage – Owners and Users are Same

As an advantage of this development toward outsourcing, highly sensitive data are now stored on systems which run in locations that are not under the control of data owners. Therefore, data confidentiality is to be put at risk.

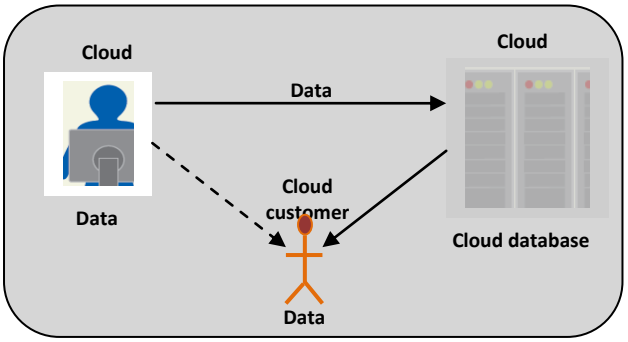

Figure 3. Data Outsourcing in Public Cloud Storage – Owners and Users are Different

There is a possibility of potential unacceptable use of database information that can be achieved by the provider itself. The traditional access control techniques may prevent data access by external users, and not by internal administrators.

V. Data Security in Cloud Computing

Data protection is a crucial security issue for most of the enterprises [32]. The main issue focused in cloud computing is data security. However, users are more concerned about the security ofthe data in the cloud. Enterprises' critical data are moved to geographically dispersed cloud infrastructure, not under the direct control of the enterprises. Moreover, data are stored in a multitenant environment and they are always in a decrypted form when used. Given the large number of issues concerning data security, many organizations want clear answers regrading security before migrating into the cloud. Data security in the cloud includes the following [33].

A. Security of data-at-rest

Users' data stored on the physical storage should not be modified. Encrypting the data may be the solution for this but in case of PaaS and SaaS, encryption of data are not always feasible and hence the probability of unauthorized access is very high.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

B. *Security of data–in-transit*

Data must be secured, while transferring between servers. It should not be viewed or changed by other user. So it requires an appropriate encryption algorithm as well as a secure protocol.

C. *Security of data during process*

Users' data should not be viewed or changed by other user at runtime.

D. *Security of data lineage*

It deals with maintaining the origin and custody of data in order to prevent tampering or to assure integrity of data. However, this is time-consuming job. Trying to provide accurate reporting on data lineage for public cloud servicesis not possible [34].

VI. Security Requirements for Cloud Storage

Security measures assumed in the cloud must be made available to the users to gain their trust [35]. There is always a possibility that the cloud infrastructure is secured with respect to some requirements and the users are looking for a different set of security mechanisms [36]. The reason why users are very anxious for the safety of their data being saved in the cloud is that they don't know who is managing it in the server of the CSP. Typical users, who use the cloud service like storing their files on the server to access it anywhere they want through internet, don't bother much about the security of their files. Those documents are common files that don't need to be secured. But in the case of big companies which have very important data to be taken care of need to have secured cloud computing system. In order to have secured cloud system, the following aspects of security parameters are considered for data protection.

A. *Authentication*

Authentication is the process of verifying a user's or other entity's identity. This is typically done to permit someone or something to perform a task. A strong authentication system ensures that the authenticators and messages of the actual authentication protocol are not exchanged in a manner that makes them vulnerable to being hijacked by an intermediate malicious node or person. That is, the information used to generate a proof of identity should not be exposed to anyone other than the person or machine it is intended for.

B. *Authorization*

Authorization is when the system decides whether or not a certain entity is allowed to perform a requested task. This decision is made after authenticatingthe identity of users. When considering an authentication system for a particular application, it is crucial to understand the type of identifier required to provide a certain level of authorization.

C. *Confidentiality*

Confidentiality is needed when the message sent or stored in the cloud contains sensitive data which should not be read by others. Hence it must not be sent in a comprehensible format. A loss of confidentiality is the unauthorized disclosure of information. Confidentiality relates to security and encryption techniques can be obtained by encrypting messages so that only intended recipients have access to read them.

D. *Integrity*

Integrity is ensuring that the data presented are true and valid. It also includes guarding against improper data modification. A loss of integrity is the unauthorized modification, insertion, or destruction of information. One way of ensuring data integrity is using simple checksums which prevent an attacker from forging or replaying messages.

E. *Non-Repudiation*

Non-repudiation is a process of ensuring that a traceable legal record is kept and has not been changed by a malicious entity. A loss on non-repudiation would result in the questioning of the transaction that has occurred. A simple example of non-repudiation is signing a contract. The signers cannot claim that they did not agree a contract, because there is an evidence that they did agree.

VII. Conclusion

Cloud gains more attention of the IT Enterprises, because of its advantages. Cloud supports on-demand computing. It reduces the cost of installing and maintaining storage servers. Though the cloud storage provides many benefits and advantages to cloud users, it has many security related issues. Security is ensured by different parameter such as authentication, authorization, confidentiality, integrity and availability. Among these parameters, confidentiality and integrity should protect the data in cloud storage. Data stored in cloud storage is controlled and monitored by the cloud providers. To protect them, it is needed that an efficient confidentiality technique for cloud data storage. Thus, it is necessary to propose a new security mechanism to protect the outsourced data in public cloud storage environment.

Reference

[1] Michael Hange, Security Recommendations for Cloud Computing Providers, Federal Office for Information Security, 2010.

[2] Armbrust M, Fox A, Griffith R, Joseph A. D, Katz R. H, Konwinski A, Lee G, Patterson D. A, Rabkin A, Stoica I, and Zaharia M., "Above the clouds: A Berkeley View of Cloud Computing", *EECS Department, University of California*, Berkeley, *Technical Report*, 2009, pp. 1-23.

[3] Zhang Q, Lu Cheng, and RaoufBoutaba, "Cloud Computing: State-of-the-Art and Research Challenges", *Springer Journal of Internet Service Application*, Volume 1, Issue 1, 2010, pp. 7-18.

[4] RajkumarBuyya, Chee Shin Yeo, SrikumarVenugopal, James Broberg and IvonaBrandic, "Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility", *Elsevier Science Publishers*, Volume 25, Issue 6, 2009, pp. 599-616.

[5] BorkoFurht, "Cloud Computing Fundamentals", *Handbook of Cloud Computing*, Chapter-1, Springer Science, Business Media, LLC, 2010, pp.1-17.

[6] Kuyoro S. O., Ibikunle F. &Awodele O., Cloud Computing Security Issues and Challenges, International Journal of Computer Networks (IJCN), Volume 3, Issue 5, 2011, pp. 247-255.

[7] Frank Gens, New IDC IT Cloud Services Survey: Top Benefits and Challenges, http://blogs.idc.com/ie/?p=730, December 15th, 2009

[8] Peter Mell and Tim Grance, "The NIST Definition of Cloud Computing", *Technical Report-800-145*, Version 15, National Institute of Standards & Technology, Gaithersburg, MD, United States, 2011.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

[9] Vaquero L M, Luis Rodero-Merino, Juan Caceres and Maik Lindner, "A Break in the Clouds: Towards a Cloud Definition",*ACM SIGCOMM Computer Communication Review*, Volume 39, Issue 1, 2009, pp. 50-55.

[10] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez, "An Analysis of Security Issues for Cloud Computing", *Journal of Internet Services and Applications*, Springer-Verlag, Volume 4, Issue 1, 2013, pp. 1-12.

[11] DananThilakanathan, Shiping Chen, Surya Nepal and Rafael A. Calvo, "Secure Data Sharing in the Cloud", *Security, Privacy and Trust in Cloud Systems*, Chapter-1: Cloud Security, Springer-Verlag Berlin Heidelberg, 2014, pp. 45-72.

[12] Khalil I. M., AbdallahKhreishah and Muhammad Azeem, "Cloud Computing Security: A Survey", *Journal of open access computers*, Volume 3, 2014, pp. 1-35.

[14] ENISA. (2009, Feb) "Cloud computing: benefits, risks and recommendations for information security." Available: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computingrisk-assessment.

[15] Cloud Computing Use Case Discussion Group. "Cloud Computing UseCases Version 3.0," 2010.

[16] B. Grobauer, T. Walloschek and E. Stöcker, "Understanding Cloud Computing Vulnerabilities," *IEEE Security and Privacy*, vol. 99, 2010.

[17] P. Kresimir and H. Zeljko "Cloud computing security issues and challenges." In PROC Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, 2010, pp. 344-349.

[18] R. K. Balachandra, P. V. Ramakrishna and A. Rakshit."Cloud Security Issues."In PROC '09 IEEE International Conference on Services Computing, 2009, pp 517-520.

[19] S. Subashini, and V. Kavitha. (2010) "A survey on security issues in service delivery models of cloud computing." *J Network ComputAppl*doi:10.1016/j.jnca.2010.07.006. Jul.,2010.

[20] M. A. Morsy, J. Grundy and Müller I. "An Analysis of the Cloud Computing Security Problem" In PROC APSEC 2010 Cloud Workshop. 2010.

[21] S. Ramgovind, M. M. Eloff, E. Smith. "The Management of Security in Cloud Computing" In PROC 2010 IEEE International Conference on Cloud Computing 2010.

[22] Cloud Security Alliance (CSA). Available: http://www.cloudsecurityalliance.org .

[23] Dr. L. Arockiam, S. Monikandan, "Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm", International Journal of Advanced Research in Computer and Communication Engineering, Volume 2, Issue 8, August 2013, pp 3064-3070.

[24] MohitMarwaha, Rajeev Bedi, "Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, 2013, pp 367-370.

[25] Siani Pearson, "Privacy, Security and Trust in Cloud Computing", HP Laboratories, HPL-2012-80R1, appeared as a book chapter by Springer, 2012, pp 1-56.

[26] K Hashizume et al., "An analysis of security issues for cloud computing", Journal of Internet Services and Applications, a Springer open journal, 2013,pp 1-13.

[27] PankajArora et al., "Cloud Computing Security Issues in Infrastructure as a Service", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, 2012.

[28] Pardeep Sharma, Sandeep K. Sood, and SumeetKaur, "Security Issues in Cloud Computing", Springer-Verlag Berlin Heidelberg, HPAGC 2011, CCIS 169, 2011, pp 36–45.

[29] L. Arockiam and S. Monikandan , "Security Framework to Ensure the Confidentiality of Outsourced Data in Public Cloud Storage", International Journal of Current Engineering and Technology, Vol.4, No.3 , June 2014, pp. 1265-1270.

[30] Richard Chow, Philippe Golle, Markus Jakobsson, RyusukeMasuoka, Jesus Molina, Elaine Shi and Jessica Staddon, "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control", *Proceedings ofACM workshop on Cloud computing security*, 2009, pp. 85-90.

[31] Fatima TrindadeNeves, Fernando Cruz Marta, Ana Maria RamalhoCorreia and Miguel de Castro Neto, "The Adoption of Cloud Computing by SMEs: Identifying and Coping with External Factors", *Proceedings of International Conference of the Portuguese Association of Information Systems - The Information Management in the age of Cloud Computing*, 2011, pp. 1-11.

[32] Raman Chawla and KirtiNagpal, "Data Security Issues & Requirements in Cloud Computing", *International Journal of Computing Science and Communication Technologies*, Volume 5, Issue 2, 2013, pp. 883-886.

[33] Shucheng Yu, Wenjing Lou, and KuiRen, "Data Security in Cloud Computing", *Handbook on Securing Cyber-Physical Critical Infrastructure*, Chapter 15, Elsevier, Morgan Kaufmann Publisher, 2012, pp. 389-410.

[34] Tim Mather, SubraKumaraswamy, and ShahedLatif, "Cloud Security and Privacy", *O'Reilly Media, Inc*, 2009.

[35] Hyun-Suk Yu, Yvette E. Gelogo and Kyung Jung Kim, "Securing Data Storage in Cloud Computing", *Journal of security Engineering*, Volume 9, Issue 3, 2012, pp. 251-260.

[36] Masayuki Okuhara, TelsuoShiozaki and Tukuya Suzuki, "Security Architecture for Cloud Computing", *FUJITSU Science and Technology Journal*, Volume 46, Issue 4, 2010, pp. 397-402.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)