Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 3, March 2016, pg.610 – 615

Security Issues in Service Models of Cloud Computing

C. Linda Hepsiba[1], J.G.R.Sathiaseelan[2]

[1]Research Scholar, Department of Computer Science, Bishop Heber College Tiruchirappalli, Tamilnadu, India

[2]Head, Department of Computer Science, Bishop Heber College Tiruchirappalli, Tamilnadu, India

[1] hepsi.linda@gmail.com, [2] jgrsathiaseelan@gmail.com

Abstract— *Cloud computing is an emerging technology for providing computing resources and storage to all kinds of users. This technology is facing lot of challenges including data and network security, interoperability, legal and compliance issues. In security issues, there exist numerous risks for the data processed or stored in the cloud environment. Cloud data are may be used by unauthorized access or users. This paper is mainly focused on security issues for cloud service models like and their solutions.*

Keywords— *Cloud Computing, Security, Service Models, Deployment Models.*

I. INTRODUCTION

According to NIST, cloud computing is stated as the model for delivering the major resources such as the storage, networks , servers ,services and applications which can be released and provisioned with minimal management effort. It has five essential characteristics they are rapid elasticity, on-demand self-service, resource pooling, broad network access and measured services. Cloud computing contains three types of delivery models or service models. which provides users to use cloud provider's applications, those delivery models supports to develop, test, deploy, host and maintain software or applications in the same Integrated Development Environment(IDE and people can use the network, storage, processor, memory and other kind of computing resources, It is provided by cloud service provider.

In the cloud computing deployment model, storage, platform, networking, platform, and software infrastructure are delivered as service sectors. The deployment models are public, private, community sand hybrid cloud. Generally, the deployment of a cloud is survived in house (Private Cloud). Public cloud is managed over a third-party location. Hybrid cloud refers to joining the two clouds like private-public cloud. Community Cloud is states to cloud implementation model, it is accessed by a specific community with several organization's infrastructure. Cloud user's security contains number of concerns, which includes the data loss, unauthorized access and the Cloud Service Providers not effectively safeguarding the cloud data.

The cloud service consumer and Cloud service provider must ensure that the cloud is safe from all kinds of exterior threats so that the user does not face any difficulty such as data theft or data loss.

Cloud Computing has many advantages such as efficiency, integration and flexibility. Additionally, it offers virtual space for users to run and deploy their applications and usage based costing. It has some demerits especially on data theft and privacy. These types of issues leads to users are reluctant to spend in cloud mainly owing to security concerns. In cloud delivery models, data or information are disturbed by Viruses, sometime information are accessed by unauthorized users. Cloud provider, ensure the confidentiality of data through assurance mechanism and contractual obligations. Once data are stored in cloud storage, cloud provider controls access to confidential data by third-party users. Cloud service provider delivers demonstrable security polices, technical solutions, user actions auditing and principle for detect and prevent malicious insider's activity to users.

II. RELATED WORK

Various security issues across service models in cloud computing, those security issues has focused by M.Sugumaran[1]. Peng Yong et al [2] provide cryptographic approaches such as group signature, XML encryption, identity-based encryption, broadcast encryption, attribute-based encryption, group encryption, search authenticator and searchable encryption, which are used to cloud storage for data security. Koorosh Goodarzi et al [3] concentrated on classical and modern cryptography algorithm for maintaining confidentiality, availability and integrity in cloud computing data storage. Bhavana Sharma [4] focused on Elliptic curve cryptography (ECC) technique for secure message integrity, non-repudiation of data, data confidentiality and message authentication, it also provides various cryptographic algorithms like symmetric and asymmetric algorithms for cloud data storage. Bollavarapu et al [5] proposed an RSA, RC4, El-Gamal, Elliptic Curve cryptography algorithms for data confidentiality and integrity in data security fundamentals. Dimitrios et al [6] provide solution for data integrity, confidentiality and authentication in cryptographic techniques for cloud storage. Neha Mishra [8] focused on data security threats and different types of cryptographic algorithms for confidential data. Alowolodu O. D et al [9] proposed Elliptic curve cryptography algorithm is used to create smaller, more efficient and faster cryptographic keys for development of secured data and secure deployment or information in cloud environment. Amounas et al [11] suggested the ECC algorithm and RSA algorithm for data confidentiality. Chandu et al [13] concentrated on RSA algorithm for data integrity in cloud environment. Gampala et al [14] explore data security in cloud using Elliptic Curve Cryptography with Digital Signature and Encryption. Lo'ai Tawalbeh et al [15] has study to concentrate on data security and privacy and suggested cryptographic techniques are increasing the confidentiality level.

III. SECURITY ISSUES IN CLOUD COMPUTING

Data Security issues are classified into three categories, they are Traditional Security Issues, Availability Issues and Third-Party Data Control Issues. Traditional Security Issues are based on network unavailability, computer attacks like viruses, warms, cookies. Traditional security concerns are cloud service providers vulnerability, authorization and authentication, expanded network attack surface. Availability, protect from Single- point-failure or Denial of Service (DOS). Third Party Data Control, third party holds the transparent data. It leads to various security and data privacy issues. It includes auditability, due diligence and contractual obligations.

Cloud Computing has some additional data security issues like, Side channel attacks, Denial of Service attacks, Mobile device attacks Data Analysis and Cheap Data, Insider and Organized Crime Cheat, Increased authentication Demands and Cost-effective of availability Side Channel attacks are occurring when virtual machines are involved during data transmission time. It affects only virtual platforms. Side Channel attacks means data leakage across virtual machine instances. Denial of Service attack's major concern is availability. It associated with Network layer within Multi-Tenant cloud Infrastructure, hypervisor and shared resources consumption are major attacks of DOS. Mobile Device attacks are more likely to affects mobile devices like, smart phones, laptops and desktops. Generally, most of the mobile devices are does not have security features. Data analysis and cheap Data are like, Gmail, Google Docs and Google Calendar. These types of data are cheap, but backups are more costly.

IV. SECURITY ISSUES IN SERVICE MODELS

Cloud computing has three service models or delivery models, they are SaaS, PaaS and IaaS. This provides different kinds of services like application platform, software and infrastructure resources. Each delivery model has its own security issues.Table.1.describes the various types of security issues in delivery models.

A. *Security Issues in SaaS*

In a conventional on-premise application deployment model, the confidential information of each organization persists to reside within the organizational boundary and which subject to its personnel security and access control policies, logical and physical. However, in the Software as a Service model, the organization information is kept beyond the organizational boundary, at the SaaS. Accordingly, the SaaS service provider should take on extra security polices to prevent data security and breaks due to security exposures in the application. Data location, Data Disposal, data Integrity, data Confidentiality, authorization and authentication, network attacks and data availability are challenges of Software as a Service delivery model.

a. *Data Location*

Data Segregations and Data Location are in cloud, it provides shared resources of cloud and data locations. Cloud provider requires disclosing of information, Sometime Natural Disasters like flooding, extreme weather and earthquake breaks the security of security of customer's data.

b. *Data Disposal*

Data disposal is refers to cloud preserving multiple copies of the single data. It leads to high availability of the data, but at the same time it is a major issue of cloud computing data storage. More copies of data are available in cloud, so deleting operation is more difficult to the cloud customers.

Security Issues	**Affected Delivery Models**			**Solutions**
	SaaS	**PaaS**	**IaaS**	
Offensive use of cloud computing	No	Yes	Yes	Strong authentication and monitoring
Data Interruption	Yes	Yes	No	High data protection
Malicious Insiders	Yes	Yes	Yes	Cloud Transparency for management and security
Denial Of Service (DOS)	No	Yes	Yes	Cloud Service provider delivers reliability and availability
Service hijacking	Yes	Yes	Yes	Provide security polices and activity monitoring
Privacy breaks	Yes	No	No	Provide communication protection
Data loss and data leakage	Yes	Yes	Yes	Use only secure API's, encryption algorithms and apply backup polices.
Shared Technology Issues	No	No	Yes	Use Access Control mechanism

Table.1. Security issues across service models

c. *Data Integrity*

Data Integrity is the basic requirement of data security because the data integrity signifies protecting information from unauthorized modifications or deletion. CSP provides mechanisms for ensuring the data integrity. The Data Integrity also guarantees for data consistency, completeness and wholeness.

d. *Data Confidentiality*

Data Confidentiality means provide data access by authorized users and systems. Strong authentication lacking is leads to illegal access. Cloud storage requires confidentiality because cloud provider should not access any user's data. Guarantees should be delivered to the customers, privacy policies, proper practices and procedures should be placed in cloud users of the data security.

e. *Authorization and Authentication*

Mash-Up authorization explains attackers can pull data from the data sources or data leakages. Sometime, centralized access control techniques are may not be favor for all kind of customer's data. Increased authentication demands allows only thin clients to accessing cloud data because it supports only limited hosting of applications and data in cloud.

f. *Network Attacks*

Social networking attacks, cloud storage stores large set of customer data. The pair of relationships between customers, suppliers, cloud providers and vendors connected to each other. It refers to data-loss.

g. *Data Availability*

Cloud storage is normally preserved multiple copies of single customer data on different servers often exist in different clouds or different locations. When a user tries to access some data or information, corresponding data are should be available to access. The software and hardware data should be available during the time of access based on demand of authorized users. Network availability is a major concern of Data Availability.

B. *Security Issues in PaaS*

The users can use the intermediate equipment to create his program and provide it to the customers over the servers and internets. The user's controls the applications that run in cloud environment, but it does not control the hardware or network substructure and operating systems. Lack of validation, anonymous sign ups and service fraud are major issues of PaaS.

C. *Security Issues in Iaas*

Cloud computing service provider delivers resources to authorized users at Pay-Per- use process it reduces the initial investment in hardware such as processing power and networking devices. IaaS provides additional capabilities like more quickly and cost-effectively data access in an internal data centers.

Reliability and physical locations are major issues in IaaS service model. But it does not provide reliability to the customer or user on the physical locations of cloud environment.

In Iaas security issues based on cloud deployment model. Issue depends on three kinds of parameters like infrastructure management and ownership, infrastructure location and Access and consumption. Public cloud deployment model has major risk during data transformation time rather than the other cloud deployment models.Table.2.describes the parameters of cloud deployment model in cloud computing.

Cloud Type	**Infrastructure**		**Access**	
	Location	**Ownership**	**Trusted**	**Untrusted**
Private	On-Premise	Organization	Yes	No
Public	Off-Premise	Third-Party providers	No	Yes
Community	Off-Premise	Third-Party providers	Yes	No
Hybrid	On and Off-Premise	Third-Party Providers and Organization	Yes	Yes

Table.2. Cloud Deployment Model

V. SOLUTIONS FOR SECURITY ISSUES

Cloud computing security has both logical and physical security challenges among all the three delivery models and service models. Cloud service provider (CSP) should be delivers an appropriate strong encryption procedure to protect the cloud storage information. Declarations, proper practices and privacy contracts should be delivered to the cloud storage users for cloud security. Cloud providers must improve the information-security governance for the purpose of security. Cloud transparency is plays a major role in cloud security because which ensure transparency within SLA. SLA is legal agreement between clients and service providers, so cloud provider can gain the trust of their clients through SLA.CPABE is a one of the technique for the confidentiality of transmitting data and storing data. A flexible and effective distribution authentication protocol is a major concern of data security in cloud storage. These kinds of protocols depend on reliability and availability of data.

VI. CONCLUSION

Cloud Computing is a model for delivering and hosting services over the internet and it is also flexible and cost-effective business model. Cloud Service Providers (CSP) delivers security polices for cloud storage. Confidentiality, Integrity and Availability are essential fundamentals in security. This paper focused on security issues in cloud computing service model architecture Finally, Cloud Computing business model still have some security issues. In the future, research will be encompassed by providing new mechanism for security issues in Cloud Environment.

REFERENCES

[1] M. Sugumaran ,BalaMurugans D. Kamalraj. "*An Architecture for Data Security in Cloud Computing*" .World Congress on Computing and Communication Technologies. 2014

[2] PENG Yong, ZHAO Wei, DAI Zhong-hua and CHEN Dong-qing."*Secure cloud storage based on cryptographic techniques*". The Journal of China Universities of Posts and Telecommunications.ELSEVIER, 2012. S1005-8885(11). pp:182-189.

[3] Koorosh Goodarzi and Abbas karimi. "*Cloud Computing Security by Integrating Classical Encryption* ". International Conference on Robert PRIDE.ELESVIER, 2014. 1877-0509. pp: 320-326.

[4] M.Bhavana Sharma. " *Security Architecture of Cloud Computing based on Elliptic Curve Cryptography(ECC)* ".International Journal of Advances in Engineering Sciences, 2013.Vol.3(3). E-ISSN: 2231-0347. Print-ISSN: 2231-2013.

[5] Swarnalata Bollavarap and Bharat Gupta. "*Data Security in Cloud Computing*". International Journal of Advanced Research in Computer Science and Software Engineering, 2014.Volume 4. Issue 3. Pp: 1208-1215.

[6] Dimitrios Zissis and Dimitrios Lekkas. "*Addressing Cloud Computing Security Issues*". ELESVIER, 2012.pp. 583-592.

[7] Jawahar Thakur and Nagesh Kumar. "*DES, AES and BLOWFISH : Symmetric key Cryptography Algorithms Simulation Based Performance Analysis*". International Journal of Emerging Technology and Advanced Engineering, 2011. Volume 1.Issue 2. ISSN: 2250-2459

[8]Neha Mishra, Shahid Siddiqui and Jitesh P.Tripathi. "*A Compendium Over Cloud Computing Cryptographic Algorithms and Security Issues*". BVICAM's International Journal of Information Technology , 2015.Vol.7 No.1. ISSN: 0973-5658.

[9]Alowolodu O.D , Alese B.K, Adetunmbi A.O., Adewale O.S and Ogundele O.S. "*Elliptic Curve Cryptography for Securing Cloud Computing Applications*". International Journal of Computer Applications, 2013. (0975-8887).

[10]Gopinath.v and Bhuvaneswaran R.S. "*Study on Secure Cloud Computing with Elliptic Curve Cryptography*". International Journal of Computer Science Issues, 2014.Vol.11. Issue 5. No2.E-ISSN:1694-0784. Print- ISSN: 1694-0814.

[11]F.Amounas and E.H.El Kinani. "*ECC Encryption and Decryption with a Data Sequence*".Applied Mathematical Sciences, 2012. Vol.6. No. 101, 5039-5047.

[12]Parsi Kalpana and Sudha Singaraju. "*Data Security in Cloud Computing using RSA Algorithm*". International Journal of Research in Computer and Communication Technology, 2012.Vol.1. Issue 4. ISSN: 2278- 5841.

[13]Chandu Vaidya and Prashant Khobragade. " *Data Security in Cloud Computing*". International Journal on Research and Innovation Trends in Computing and Communication, 2015. Volume ,3. Issue.5. ISSN: 2321-6169. pp: 167-170.

[14]Veerraju Gampala, Srilakshmi Inuganti and Satish Muppidi. "*Data security in Cloud Computing With Elliptic Curve Cryptography*". International Journal of soft Computing and Engineering, 2012. Volume.2. Issue.3.ISSN: 2231-2307.

[15] Lo'ai Tawalbeh1, , Nour S. Darwazeh, Raad S. Al-Qassas and Fahd AlDosari1. "*A Secure Cloud Computing Model based on Data Classification*". First International Workshop on Mobile Cloud Computing Systems, Management, and Security.ELESVIER, 2015. 1153 – 1158.

[16] Prince Jain, "*Security Issues and their Solution in Cloud Computing*", International Journal of Computing & Business Research ISSN (Online):2229-6166.

[17]Hashizume et al. "*An Analysis of Security Issues for Cloud Computing*", Journal of Internet Services and Applications. Springer, 2013.

[18]Osama Harfoushi, Bader Alfawwaz, Nazeeh A, Ghatasheh, Ruba Obiedat, Mua'ad M. Abu-Faraj and Hossam Faris,"*Data Security Issues and Challenges in Cloud Computing: A Conceptual Analysis and Review*" .Communications and Network, 2014, 6, 15-21.

[19]A.P.Bhutada and S.L.Magar. "*Executing DES Algorithm in Cloud Data Protection*". International Journal of Innovative Research in Engineering and Technology**.**Leiutis, 2015. Volume.1.Issue.1.

[20]Shivali munjal and Ramandeep singh. " *Data Security in Cloud Computing*" IJSER, 2014. Volume.5, Issue.3,ISSN :2229-5518.

[21]M.Mohamed Sirajudeen and Dr. K. Subramanian, "*Security Issues on Data Transfer under Clouds – An Overview*" September – October 2014 International Journal of Information Technology Infrastructure. Volume.3. No.5.ISSN: 2320 2629.

[22]Kuyoro S.O,Ibikunllef and Awodele.O,"*Cloud Computing security issues and challenges*",IJCN,2011.

[23]Mohammed A.Alzain,Ben Soh and Eric Pardede, "*A survey on data security in cloud Computing*,"Journal of software, May 2013.

[24]M.Ali, S.U.Khan and A.V.Vasilakos. "*Security in Cloud Computing: Opportunities and Challenges*". Information Sciences.ELESVIER, 2015.INS 11378.

[25] Ramgovind S, Eloff MM and Smith E. "*The Management of Security in Cloud Computing*". IEEE. 2010. 978-1-4244-5495.