International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 2 Issue 8
August 2015

Security Issues and Measures for Cloud Users: A Survey Paper

Tiyasa Gupta[1] , Prince Paul[2], RamachandraTawker[3], ShoneySebastian[4]
Department of Computer ScienceChrist University, Bengaluru

Abstract**—***Cloud computing is one of today's most developing and promising innovation in view of its capacity to chop down processing expenses. It empowers clients to store their information and data and utilize astounding cloud applications and administration with no weight of neighborhood equipment and programming foundation. From the previous couple of years, distributed computing has risen up out of being only a business thought to one of the quickest developing field in the IT division. As it is being utilized by tremendous number of individuals for their business and additionally individual needs, there is a noteworthy security sympathy toward the cloud suppliers, i.e. to give most extreme security to the cloud clients. As all the data is kept in a solitary spot i.e. cloud, it will be less demanding for the programmer to get entrance. This paper gives an outline about distributed computing, its clients, the security dangers included with the cloud clients and a few proposals against cloud security issue.*

IndexTerms**—*****Cloud Computing, Security Issues, Measures,Survey***

I. INTRODUCTION

Cloud refers to a metaphor to state web as a space where computing is being pre-installed and can be used as a service- Software, Infrastructure, Platform, Application, Storage etc. To the Users of cloud, it is Pay-Per-Use-On-Demand mode that can easily gain access to the IT resources through the web.

IT services include network, storage, server, application etc. and can be deployed efficiently without much cost and management. It is easy and cheap to use cloud services.

There are mainly three components of cloud i.e. Client- Thin, Thick and Mobile, Datacenters and Distributed Servers

The services offered my cloud to its users are [11]:

Software as a Service (SaaS): A web application is hosted via internet for the users as a service. The user doesn't have to worry about maintaining or supporting it.

Platform as a Service (PaaS): It provides all the necessary assets required to build an applications and service from the web, without having to download or install the software.

Infrastructure as a Service (IaaS): It provides infrastructure components such as computing power or storage capacity. The user just buys the operating system rest the cloud provider manages the system's CPU, memory and processing

Database as a Service (DaaS): It provides database service so that one can evade the complexity and cost of running one's own database.

There are three deployment models of cloud [10]:

Public cloud: It is owned by the cloud service providers and it also offers a very high level of efficiency in shared resources.

Private cloud: It functions only for one organization on a private network and is highly secure.

Hybrid cloud: It is the combination of private and public deployment models. Here some specific resources are run in the public cloud while some others are used in a private cloud in the organization and so this in turn provides increased efficiency.

But one major concern that comes in the way for a user of cloud is its security. There are many scholarly articles, researches and periodicals focusing on different cloud security issues and solutions or measures to curb the issues. This survey paper presents an insight of various issues and security measures that come in the way for a cloud user mainly of public cloud because it is most vulnerable to attacks.

II. CLOUD SECURITY

As thousands of users are added to cloud every day, there are lots of data that needs to be maintained. Maintaining includes storing as well as securing the data from falling into wrong hands. When a client uploads some data into cloud, the data leaves from the client and goes to a third party. It is the responsibility of the cloud providers to make sure that the data is not hampered by any means. Even the client should look for a good provider to store his data. These days many cloud providers came into existence. It is required to have proper knowledge before giving them the data. There are different security measures to protect the data on the cloud. It is a big responsibility of the providers because if they don't keep the data secure, they will lose their customers. In this era of competition, all the

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 2 Issue 8
August 2015

providers do their best to make the cloud as secure as possible.

III. RELATED WORK

The various security issues and the measures to manage the issues as mentioned in the paper [1] is as follows:

Gartner's seven security issues which cloud clients should advert which are mentioned in the paper arePrivileged user access, Regulatory compliance, Data location, Data segregation, Recovery, Investigative support and Long-term viability.

Other user security issues mentioned includes Data leakage and Cloud Security issues such asAttacks in cloud and DDoS attacks in cloud.

Various solutions for the security issues mentioned areAccess Control which can be done by the six Control Statements namely Control access to information, Manage user access rights, Encourage good access practices, Control access to network services, Control access to operating systems and Control access to applications and systems.

Incident Countermeasure and response which is done to achieve flexibility, scalability, and efficiency usage of available resources, cloud providers must face major challenges in the area adaptability and workload analysis and prototypes lies in these analysis and adaptation components like Partitioning, Migration and Workload Analysis and Allocation

The various security issues and the measures to manage the issues as mentioned in the paper [2] is as follows:

Various user security issues mentioned are Network security issues such as Transfer security,Firewalling andSecurity configuration.Different Interfaces such as API, Administrative interface, User interface and Authentication, Data security issues related to Cryptography, Redundancy and Disposal, Virtualization issues such as Isolation, Hypervisor vulnerabilities, Data leakage, VM identification, Cross-VM attacks, Governance issues like Data control, Security control and Lock-in, Compliance issues such as Service Level Agreements (SLA), Loss of service, Audit and Service conformity, Legal issues such as Data location, E-discovery, Provider privilege and Legislation

Organizations working for Security Frameworks:

ENISA- ENISA is an agency responsible for achieving high and effective level of network and information security within the European Union. They published a report in which security risks are divided in four categories namely Policy and organizational for issues related to governance, compliance and reputation, Technical for issues derived from technologies used to implement cloud services and infrastructures, such as isolation, data leakage and interception, denial of service attacks, encryption and disposal, Legal for risks regarding jurisdictions, subpoena and e-discovery and Not cloud specific for other risks that are not unique to cloud environments, such as network management, privilege escalation and logging.

CSA- CSA is an organization led by a coalition of industry practitioners, corporations, associations and other stakeholders, such as Dell, HP and eBay. One of its main goals is to promote the adoption of best practices for providing security within cloud computing environments.

CSA documents are The security guidance which establishes thirteen security domains namely, Governance and risk management, Legal issues, Compliance and audit, Information management and data security, Portability and interoperability, Traditional security, business continuity and disaster recovery, Data center operations, Incident response, notification and remediation, Application security, Encryption and key management, Identity and access management, Virtualization and Security as a service

Out of the top threats in cloud computing, seven threats were selected are Abuse and nefarious used of cloud computing, Insecure application programming interfaces, Malicious insiders, Shared technology vulnerabilities, Data loss and leakage, Account, service and traffic hijacking and Unknown risk profile.

The various security issues and the measures to manage the issues as mentioned in the paper [3] is as follows:

Various user security issues mentioned includescompany has violated the law (risk of data seizure by (foreign) government), Storage services provided by one cloud vendor may be incompatible with another vendor's services if user decides to move from one to the other (e.g. Microsoft cloud is incompatible with Google cloud), who controls the encryption/decryption keys? Logically it should be the customer, ensuring the integrity of the data (transfer, storage, and retrieval) really means that it

changes only in response to authorized transactions. a common standard to ensure data integrity does not yet exist, some government regulations have strict limits on what data about its citizens can be stored and for how long, and some banking regulators require that customer's financial data remain in their home country, customers may be able to sue cloud service providers if their privacy rights are violated, and in any case the cloud service providers may face damage to their reputation. Concerns arise when it is not clear to individuals why their personal information is requested or how it will be used or passed on to other parties. With the cloud model control physical security is lost because of sharing computing resources with other companies. No knowledge or control of where the resources run. The dynamic and fluid nature of virtual machines will make it difficult to maintain the consistency of security and ensure the audit ability of records. In case of Payment Card Industry Data Security Standard (PCI DSS) data logs must be provided to security managers andregulators.Users must keep up to date with application improvements to be sure they are protected.

Various solutions for the security issues mentioned are includes Investigation Support, Network Security, Encryption Algorithm, Backup, Customer satisfaction.A Security Management Model is also discussed which includes topics such as Security management (People), Security governance, Software-as-a-Service (SaaS) security , Risk management, Risk assessment, Data governance, Virtual machine security, Disaster recovery, Third party risk management, Vulnerability assessment, Security image testing, Security awareness, Change management, Data security, Data privacy, Application security, Identity Access Management (IAM), Education and training, Physical security and Policies and standards.

The various security issues and the measures to manage the issues as mentioned in the paper [4] is as follows:

Various user security aspects mentioned are Availability, Confidentiality, Privacy, Data Integrity, Identity and Access Management (IAM), Control, Audit, Compliance and Security-as-a [cloud] Service.

Various user security issues mentioned are Threats to cloud computing discovered by "Cloud Security Alliance" (CSA) which includes Abuse and Nefarious Use of Cloud Computing, Insecure Application Programming Interfaces, Malicious Insiders. Some other issues mentioned are Shared Technology Vulnerabilities, Data Loss/Leakage, Account, Service & Traffic Hijacking, some Security Problems Concerning Location of the Cloud Systems such as Multi-location of the private data, Multi-location of the service provider, Data combination and commingling, Restrictions on techniques and logistics and Data transfer across the borders. Other Cloud Challenges Inherited from Network Concept like SQL injection attacks, Cross Site Scripting (XSS) attacks, Man in the Middle attacks (MITM), Sniffer Attacks, Reused IP Addresses, Security Concerns with the Hypervisor, Denial of Service Attacks, Cookie Poisoning, Distributed Denial of Service Attacks, CAPTCHA Breaking and Google Hacking.

It also includes some Inevitable Cases of Information Disclosure like Electronic Communications Privacy Act (ECPA), USA PATRIOT Act (UPA), Health Insurance Portability and Accountability Act (HIPAA), Fair Credit Reporting Act (FCRA), Video Privacy Protection Act (VPPA), Gramm Leach Bliley Act (GLBA) and Cable Communications Policy Act (CCPA)

Some other Common Security Threats include Investigation, Data Segregation, Long-term Viability, Compromised Servers, Regulatory Compliance, Security Issues in Virtualization and Identity Management

Various solutions for the security issues mentioned include some general security counter measures such as Architecture security, Data Security, Protection from attacks at various levels, Using Mirage Image Management System, Using Client Based Privacy Manager and Transparent Cloud Protection System (TCPS) and also few countermeasures for Challenges Inherited from Network Concept are SQL injection attacks, Cross Site Scripting (XSS) attacks, Man in the Middle attacks (MITM), DNS Attack, Sniffer Attacks, Security Concerns with the Hypervisor, Denial of Service Attacks, Cookie Poisoning, Distributed Denial of Service Attacks, CAPTCHA Breaking and Google Hacking. Some other countermeasures for CAS proposed threats includes Confronting Abuse and Nefarious Use of Cloud Computing, Confronting Insecure Application Programming Interfaces, Confronting Malicious Insiders., Confronting Shared Technology

Vulnerabilities, Confronting Data Loss/Leakage and Confronting Account, Service & Traffic Hijacking.

The various security issues and the measures to manage the issues as mentioned in the paper [5] is as follows:

Various user security aspects mentioned are the traditional security challenges such as Authentication and authorization, Availability, Data confidentiality and Virtual Machine Security.

Some Cloud Specific Security Challenges are Information Security, Network Security, Resource Locality and Cloud standards.

Possible ‘‘Inter-cloud’’ standards in the following domains are needed to increase cloud interoperability and free data movement among clouds includes Network architecture, Data format, Metering and billing, Quality of Service, Resource provisioning, Security, identity management and privacy.

Other issues include Data Segregation, Data Access, and Web application security, Data breaches, Backup, Identity management and sign-on process.

Various solutions for the security issues mentioned are Open Authorization, Two Factor Authentication, OAuth, Data Dispersion, Attribute based Proxy Re-Encryption, Reconfigurable distributed virtual machine, Survey on Virtual Machine Security, Information Security Risk Management Framework, Network Security for virtual machines, Network Security Sandbox, IEEE Cloud Computing Standard Study Group, ITU Cloud Computing Focus Group, Cloud Security Alliance (CSA), Multi-user access policies, Data Access Management, Web Application Scanners, Agentless Method for data Backup and Recovery and CSA’s Identity and Access Management Guidance.

The various security issues and the measures to manage the issues as mentioned in the paper [6] is as follows:

Various user security issues mentioned are XML Signature, Browser Security which includes The Legacy Same Origin Policy, Attacks on Browser-based Cloud Authentication in which two enhancements can be added to the browser security API namely XML Encryption and XML Signature, Future Browser Enhancements Secure Browser-based Authentication.

Four methods to protect SAML (Security Assertion Markup Language is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider) tokens with the help of TLS (Transport Layer Security) includes TLS Federation, SAML 2.0 Holder-of-Key Assertion Profile, Strong Locked Same Origin Policy, TLS session binding.

Some other issues include Integrity and Binding Issues such as Cloud Malware Injection Attack and Metadata Spoofing Attack, Flooding Attacks like Direct Denial of Service, Indirect Denial of Service and Accounting and Accountability.

The various security issues and the measures to manage the issues as mentioned in the paper [7] is as follows:

Various user security issues mentioned are Data Issues such as Data Integrity, Data Stealing, Data Loss, Data Location.

Some other issues are Privacy issues, Infected Application and Security issues at both User and Provider’s level

Various solutions for the security issues mentioned includes Verifying the access controls, Control the consumer access devices, Monitor the Data Access, Share demanded records and verify the data deletion, Security check events.

The various security issues and the measures to manage the issues as mentioned in the paper [8] is as follows:

Various user security issues mentioned are Abuse and Nefarious Use of Cloud Computing, Insecure Application Programming Interfaces, Malicious Insiders, Shared Technology Vulnerabilities, Data Loss/Leakage, Account, Service & Traffic Hijacking and Unknown Risk Profile

Various solutions for the security issues mentioned areUnderstand the cloud, Demand Transparency, Reinforce Internal Security, Consider the Legal Implications and Pay attention.

Some issues to be clarified before adopting Cloud Computing areUser Access, Regulatory Compliance, Data location, Data Segregation, Disaster Recovery Verification, Disaster Recovery and Long-term Viability.

The various security issues and the measures to manage the issues as mentioned in the paper [9] is as follows:

Various user security issues mentioned are Virtual Machine Attack, Malware Injection Attack, Insecure cryptographic storage, Session riding and Hijacking,

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 2 Issue 8
August 2015

Vendor lock-in, Insecure APIs, Denial of service attack and Data loss and leakage.
Various solutions for the security issues mentioned arePrivacy Enhanced Data Outsourcing in the Cloud, Privacy-preserving access control for cloud computing, public remote integrity checks for private data, Privacy enhanced keyword search in clouds.

IV. EVALUATION OF ISSUES AND MEASURES

Reference	Research theme	Issues discussed	Proposed solutions
[1] Farzad	Cloud computing security threats and responses	Gartner's Seven Security Issues, Attacks in cloud and DDoS attacks in cloud	Access control using six control statements
[2] Nelson	A quantitative analysis of current security concerns and solutions for cloud computing	Network Security Issues, Governance Issues	Organizations working on Security Frameworks
[3] Rajesh	An Overview and Study of Security Issues & Challenges in Cloud Computing	Incompatibility in storage services, Control of encryption/decryption keys	Investigation Support, Encryption Algorithm, Security Management Model
[4] Vahid	Security threats and countermeasures in cloud computing	User security aspects, Threats to Cloud Computing discovered by CSA	Mirage Image Management System, Client Based Privacy Manager, Transparent Cloud Protection System (TCPS)
[5] Rashmi	Securing software as a service model of cloud computing: Issues and solutions	Authentication, Authorization, Inter-Cloud Standards	Open Authorization, Two factor authentication, IEEE Cloud Computing Standard Study Group
[6] Meiko	On technical security issues in cloud computing	Browser Security, Integrity and Binding Issues	Transport layer Security
[7] Prince	Security Issues and their solution in cloud computing	Security Issues at both user and provider's level, Data Issues	Monitor Data Access, Security Check events.
[8] Anthony	An overview of the security concerns in enterprise cloud computing	Abuse and Nefarious Use of Cloud Computing, Insecure Application Programming Interfaces	Demand transparency, Issues to be clarified before using cloud
[9] Kachavimath	Security issues in cloud computing: A Study	Virtual Machine Attack, Session Riding and Hijacking	Privacy Enhanced Data Outsourcing in the Cloud, Privacy-preserving access control for cloud computing

V. CONCLUSION

Cloud Technology is growing in a rapid rate and is widely accepted by many organizations as well as individual. It has gained popularity due to its efficient performance in a very low cost. Though it offers lot of services, it has some security issues which needs to be taken care of as thousands of people are using cloud services. The organizations working for the security of the cloud services should address the key security issues like confidentiality, integrity, authentication etc. The Chief Information Officers (CIOs) and Chief Security Officers (CSOs) of the cloud user and provider sides need to understand and address the risk and security issues in detail before actually benefiting its high-end computing power. Proper laws should be enforced and followed so that the user security is ensured.

REFERENCES

[1] Sabahi, Farzad. "Cloud computing security threats and responses."Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on. IEEE, 2011.
[2] Gonzalez, Nelson, et al. "A quantitative analysis of current security concerns and solutions for cloud computing." Journal of Cloud Computing 1.1 (2012): 1-18.
[3] Piplode, Rajesh, and Umesh Kumar Singh. "An Overview and Study of Security Issues & Challenges in Cloud Computing." International Journal of Advanced Research in Computer

Science and Software Engineering 2.9 (2012): 115-120.

[4] Ashktorab, Vahid, and Seyed Reza Taghizadeh. "Security threats and countermeasures in cloud computing." International Journal of Application or Innovation in Engineering & Management (IJAIEM) 1.2 (2012): 234-245.

[5] Rashmi, Dr G. Sahoo, and Dr S. Mehfuz. "Securing software as a service model of cloud computing: Issues and solutions." International Journal on Cloud Computing: Services

[6] Jensen, Meiko, et al. "On technical security issues in cloud computing." Cloud Computing, 2009. CLOUD'09. IEEE International Conference on. IEEE, 2009.

[7] Jain, Prince. "Security Issues and their solution in cloud computing."International Journal of Computing & Business Research (2012).

[8] Bisong, Anthony, and M. Rahman. "An overview of the security concerns in enterprise cloud computing." arXiv preprint arXiv: 1101.5613 (2011).

[9] V.Kachavimath, Amit and Somangoudar Shruti. “Security issues in cloud computing: A Study” IJEDR. Volume 3, Issue 2 ISSN: 2321-9939 (2015)

[10] Parsi, Kalpana, and M. Laharika. "A Comparative Study of Different Deployment Models in a Cloud." International Journal of Advanced Research in Computer Science and Software Engineering 3.5 (2013): 512-515.

[11] Charan, N. Ram Ganga, S. Tirupati Rao, and P. V. S. Srinivas. "Deploying an Application on the Cloud." International Journal of Advanced Computer Science and Applications 2.5 (2011).