Asian Journal of Computer Science and Technology
ISSN: 2249-0701 Vol.8 No.S1, 2019, pp. 80-83

Security Threats in Cloud Computing

J. VimalRosy[1] and S. Britto Ramesh Kumar[2]
[1]Head, Department of Computer Science, Soka Ikeda College of Arts and ScienceforWomen, Tamil Nadu, India
[2]Assistant Professor, Department of Computer Science, St.Joseph's College, Tamil Nadu, India
E-Mail: robi_rosij@rediffmail.com,brittork@gmail.com

Abstract **- Day by day witnesses a wide development of information technology in the use of cloud computing, and its services shape its architecture. It is indeed, that replaces the former attempts to enrich the security strategy in cloud computing. Security is one of the major issues in the cloud computing environment. In this paper we investigate about security threads and possible solution for cloud. The paper is categorized as follows: Section I describes the cloud computing overview. Section II describes the security threats and challenges in cloud computing. Section III describes the Obstacles and vulnerabilities that can be carried out to cloud environments. Section IV describes the possible solution of the issues. Section V concludes the paper with a cloud computing security.**
Keywords: **Cloud Computing, Cloud Security**

I. INTRODUCTION

Cloud computing is an umbrella term used to refer to Internet based development and services. The cloud is a metaphor for the Internet. A number of characteristics define cloud data, applications services and infrastructure:

1. Remotely hosted: Services or data are hosted on someone else's infrastructure.
2. Ubiquitous: Services or data are available from anywhere.

Cloud computing uses three service model: software as a service (SaaS), platform as a service (PaaS) and intrastructure as a service (IaaS).

A. Software as a Service (Saas)

SaaS is a model of software deployment where an application is hosted as a service provided to customers across the Internet. SaaS is generally used to refer to business software rather than consumer software, which falls under Web 2.0.

By removing the need to install and run an application on a user's own computer it is seen as a way for businesses to get the same benefits as commercial software with smaller cost outlay. Saas also alleviates the burden of software maintenance and support but users relinquish control over software versions and requirements.

Benefits of the SaaS model include:

1. Easier administration
2. Automatic updates and patch management
3. Compatibility: All users will have the same version of software.
4. Easier collaboration, for the same reason
5. Global accessibility.

Examples:Google docs, Microsoft- office 365,p rezi.com

B. Platform as a Service (Paas)

Your computing platforms, such as operating system, programminglanguage execution environment, database, web server etc., are all based in the Cloud. PaaS has several advantages for developers.

1. Operating system features can be changed and upgradedfrequently
2. Teams can work together on software development regardless ofdistance
3. Services can be obtained from diverse sources that cross internationalboundaries.
4. Initial and ongoing costs can be reduced by using a singlevendor
5. Multiple projects can use the samedevelopers

Examples:AWS Elastic beanstalk, SalesForce.com Google App Engine IBM.

C. Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS) Infrastructure as a Service is a single tenant cloud layer where the Cloud computing vendor's dedicated resources are only shared with contracted clients at a pay-per-use fee. This greatly minimizes the need for huge initial investment in computing hardware such as servers, networking devices and processing power. They also allow varying degrees of financial and functional flexibility not found in internal data centers or with collocation services, because computing resources can be added or released much more quickly and cost-effectively than in an internal data center or with a collocation service. IaaS and other associated services have enabled startups and other businesses focus on their core competencies without worrying much about the provisioning and management of infrastructure. IaaS completely abstracted the hardware beneath it and allowed users to consume infrastructure as a service without bothering anything about the underlying complexities. The cloud has a compelling value proposition in terms of cost, but 'out of the box' IaaS only provides basic security (perimeter firewall, load balancing, etc.) and applications moving into the cloud will need higher levels of security provided at the host.

D. Characteristics of Iaas Include

1. Utility service and billing model.
2. Automation of administrative tasks.

3. Dynamics caling.
4. Desktop virtualization.

Examples: Aws. amazon.com , EC2, S3,Cloud.google.com, rackspace.com. www.windowsazure.com

E. Three Cloud Computing Deployment Models

Fig.1 Deployment models and service models of the cloud computing

F. Public Cloud

Public cloud or external cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self service basis over the Internet, via web applications/web services from an off-site third-party provider who bills on a fine-grained utility computing basis. The cloud infrastructure is made available to the general public or a large industry group, and is owned by an organization selling cloud services. Examples: Amazon Elastic-Compute-Cloud,IBM's BlueCloud, Sun Cloud, Google AppEngine.

G. Private Cloud

The infrastructure of a private cloud is only used by a single customer. It can be managed by the customer or a service provider. It can be located in the client company's premises or at the provider. For example, using a private cloud ensures that the allocated hardware resources will never be shared by two different customers.

H. Hybrid Cloud

A hybrid cloud environment is the combination of public andprivatecloudwheretheinfrastructure partially hosted inside the organization and externally in a public cloud . For example, an organization might use Amazon Simple Storage Service (Amazon S3) as public cloud service to records their data but at the same time continue in-house storage for instant access operational customer data. Hybrid storage clouds are often valuable for record keeping and backup function. It is a good approach for a business to take advantage of the cost effectiveness and scalability.

I. CommunityCloud

Acommunitycloud can be recognized where a number of organizations have comparable necessities and very willing to share infrastructure so as to take in the benefits of cloud computing. Here costs increase than a public cloud and sometimes can be more expensive but may offer a higher level of privacy and security.

II. THREATS IN CLOUDCOMPUTING

A threat can cause damage to a system and create a loss of confidentiality, availability or integrity. Threats can be malicious such as the intentional modification of sensitive information. Threats Cloud computing faces just as much security threats that are currently found in the existing computing platforms, networks, intranets, internets in enterprises. These threats, risk vulnerabilities come in various forms. This paper reviews XML Signature, Browser Security, Data Breaches, account Hijacking and multitenancy threats.

1. Abuse and nefarious use of cloud computing
2. Insecure interfaces &API's
3. Unknown risk profile
4. Malicious insiders
5. Shared technology issues
6. Data loss or leakage
7. Account or service hijacking

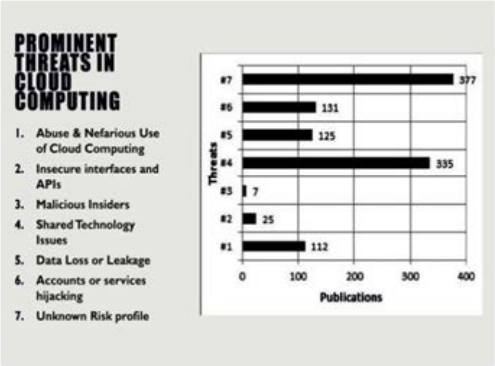

Fig. 2 Prominent threats in cloud computing

1. Abuse and Nefarious Use of Cloud Computing: IaaS providers offer the illusion of unlimited capacity with a frictionless Legistration process for cloud services. The abuse of relative anonymity by criminals to target IaaS vendors also.

2. Insecure Interfaces &API's: Cloud computing providers APIs to manage it provisioning, management etc are done using these interfaces. The security depends on APIs. From authentication and access to encryption are designed to protect against accidental and malicious attempts. The new layered API increases risk and relinquish credentials to third parties.

3. Unknown Risk Profile Description: The tenet of cloud computing is the reduction of hardware and software ownership to allow their business strengths. This has clear financial and operational benefits against security concerns by groups losing security ramifications.

4. Malicious Insiders: Insiders who exploit cloud vulnerabilities gaining unauthorized access to confidential data or carry out attacks against its own employer's IT infrastructure.

5. Shared Technology Issues: Not all of the current infrastructure provide for shared usage. To ensure that customers don't threat on each other's resource, monitoring and strong compartmentalization is required.

6. Data Loss or Leakage: To compromise data, deletion or alteration of records is an obvious example. Unlinking a record may render itunrecoverableandalossofanencoding key may result destruction. This threat increases in the cloud is unique and dangerous.

7. Account orService Hijacking: Account of service hijacking asphishing, fraud and exploitation of software vulnerabilities amplifies the impact of and eavesdrop our activities and redirect to a illegitate area which is new for the attacker.

III. OBSTACLES ANDVULNERABILITY

Obstacles to and opportunities for adoption and growth of cloud computing**.** The obstacles with hinder the growth of cloud computing are listed below table I.

TABLE I OBSTACLES AND VULNERABILITY

Obstacle	Opportunity
Availability of Service	Use Multiple Cloud Providers to provide Business Continuity; Use Elastic toDefend Against DDOS attacks
Data Lock-In	Standardize APIs; Make compatible software available to enable SurgeComputing.
Data Confidentiality and Auditability	Deploy Encryption, VLANs, and Firewalls; Accommodate National Laws viaGeographical Data Storage
Data Transfer Bottlenecks	FedExing Disks; Data Backup/Archival; Lower WAN Router Costs; Higher Bandwidth LAN Switches
Performance Unpredictability	Improved Virtual Machine Support; Flash Memory;Gang Scheduling VMs for HPC apps
Scalable Storage	Invent Scalable Store
Bugs in Large-Scale Distributed Systems	Invent Debugger that relies on Distributed VMs
Scaling Quickly	Invent Auto-Scaler thatrelies on Machine Learning; Snapshots to encourage CloudComputing on conservationism.
Reputation Fate Sharing	Offer reputation-guarding services like those for email.
Software Licensing	Pay-for-bulk: use sales

IV. POSSIBLE ISSUES ANDSOLUTION

Many researchers have been investigated auditing the integrity of data of untrusted servers. The first publicly verifiable PDP scheme which employed RSA-based homomorphic authenticators and sampled several data blocks rather than the whole data file to audit the outsourced data. Next it is proposed a publicly verifiable POR scheme with a comprehensive proof of security under the POR model and gave similar constructions for publicly verifiable remote data integrity check, which adopted the BLS based homomorphic authenticators.

A. Definition of System Model

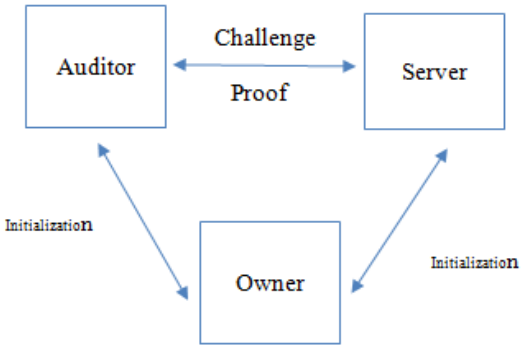

Fig.3 System model

B. Solution

Further research followed an auditing framework for cloud storage systems introducing an efficient and privacy preserving auditing protocol which paved way to extend auditing protocol to support the data dynamic operations. It is efficient and provably secure in this model. Then extend the auditing for both multiple owners and multiple clouds without using any trusted organizer. However, due to a large number of data tags the auditing protocol incurs a heavy storage overhead on the server. It is impossible that system to support the batch auditing for multiple owners so that their scheme applies include the mask technique to ensure the data privacy. We can secure our data like this in future.

V. CONCLUSION

By presenting this paper, thought here are many advantages and benefits of using a cloud system, a number of issues block our way of certain users. For that purpose, a selection of issues of cloud computing security, such as Abuse and nefarious use of cloud computing, Insecure interfaces & API's, Unknown risk profile description, Malicious insiders, Data Loss or Leakage, Account or Service hijacking are presented in this paper. Even the data residing inside the cloud is vulnerable to attacks. In this paper, we presented various aspects of security in cloud and the challenges associated on different parts of cloud infrastructure. So, we identified them and evaluated exiting possible solutions to this issue.

REFERENCES

[1] Yang and X. Jia, "Data storage auditing service in cloud computing: challenges, methods and opportunities,"*WorldWideWeb*,Vol.15,No.4,pp.409–428, 2012.

[2] Y. Zhang and M. Blanton, "Efficient dynamic provable possession of remote data via balanced update trees",*in Proceedings of the 8th ACMSIGSAC Symposium on Information, Computer and Communications Security, ASIACCS*, pp. 183–194, ACM, 2013.

[3] Guan, K. Ren, F. Zhang, F. Kerschbaum, and J. Yu, "Symmetric- Key Based Proofs of Retrievability Supporting Public Verification", *Springer International Publishing*,pp.203–223,2015.

[4] V.K.Reddy, L. Said, B. Sengupta, M. Chetlur, J.P.Costantino, A. Gopinath, S. Flynt, P. Balunaini, and S. Vedula, "Personalized learning pathways: Enabling intervention creation and tracking", *In IBM Journal of Researchand Development*, Vol. 59, No. 6, November 2015.

[5] M. Sarkar, and T. Chatterjee, *International Journal on Network Security*, Vol. 5, No. 1, Jan 2014.

[6] R. Chaves and L. Sousa. "Improving residue number system multiplication with more balanced moduli sets and enhanced modular arithmetic structures",*Computers &Digital Techniques,IET*, Vol.1, No.5, pp. 472-480,Sept.

[7] M.Re, A. Nannarelli, G. C. Cardarilli, and R.Lojacono,"FPGARealization of RNS to binary signed conversion architecture",*In 2001 IEEE International Symposium On Circuitsand Systems*, Sydney, Australia, pp. 6–9 May 2001.

[8] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "*Scalable and Efficient Provable Data Possession," Proc. ofSecureComm*'08, pp. 1–10, 2008.

[9] Wentao Liu, *Research on Cloud Computing Security Problem and Strategy*, 978-1-4577-1415-31121 ©2012 IEEE

[10] NIST defmition of Cloud. NIST 500-292, *NIST Cloud Computing ReferenceArchitecture.*