ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
Indian Journal of Science and Technology, *Vol 9(45), DOI: 10.17485/ijst/2016/v9i45/105325, December 2016*

A Review on Cloud Computing Technologies and Security Issues

K. Padmaja[1] and R. Seshadri[2]

[1]Department of Computer Science and Engineering, Sri Venkateswara University College of Engineering, Sri Venkateswara University, Tirupati – 517 502, Andhra Pradesh, India; padmajaskrishna@gmail.com

[2]Director of University Computer Center, Sri Venkateswara University College of Engineering, Sri Venkateswara University, Tirupati – 517 502, Andhra Pradesh, India; ravalaseshadri@gmail.com

Abstract

This study provides an overview of technologies, deployment models and issues of security present in the cloud computing industry. A new model needs to be framed to enhance the characteristics of an existing model.

Keywords: Cloud Computing Technologies, Confidentiality, Network Transport Security, Open Security Architecture, Privacy-Preservability

1. Introduction

Clouds can be ramped up of resources either physical or virtualized over centralized or propagated data centres. A cloud comprises various types of workloads like batch style backend jobs and client facing applications. In Cloud, numerous inevitable failures (hardware/ software) regained by way of quick delivery of either virtual or physical machines. In real time, cloud system supervises resource utilization to permit balanced allocations of resources when required. Need for distributed and cloud computing has been incremented due to the role of virtualization technology. Multiple Virtual Machines (VMs) are multiplexed in the same hardware machine by the usage of virtualization technology. The thought behind virtualization is to assort hardware from the software to render better performance. Hardware or software services, namely Central Processing Unit (CPU), storage, Operating System (OS) and software libraries can be virtualized in functional layers[1].

Cloud computing gives a comprehensive economic gain, instead of possessing and managing their own systems, end users share centralized pond of resources[2]. These days, cloud computing promoted as industrial infrastructure, rids of retaining computer hardware. Clouds are alternatives to cluster, grids and supercomputer[3].

Cloud computing is a multitenant technology. It is 5-4-3 model i.e., 5 essential characteristics,4 deployment models and 3 popular service models which are provided as services by provider's from the cloud. Metered assistance, speedy elasticity, on-demand self provider, resource pooling and extensive network connection, these are five characteristics of cloud computing. Public, private, hybrid and community cloud comes under types

*Author for correspondence

of clouds. Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) are three popular service models of cloud.

2. Cloud Computing Technologies

2.1 Microsoft Cloud Technologies

Microsoft is a principal supplier of cloud technologies and applications with results matches with all sorts of business needs. It gives all sorts of services whether it is PaaS, IaaS on the other hand SaaS. In the event that we discuss Infrastructure-as-a-Service, Microsoft gives the windows server and system canter. Furthermore, in case of PaaS it give Windows Azure; with this, user can easily construct, host and scale applications in Microsoft datacenter without in advance costs simply pay for what you use. Different PaaS administrations are SQLSERVER and VISUAL STUDIO. Microsoft also provides office365, share point servers, dynamic Customer Relationship Management (CRM) and trade server as SaaS. Microsoft Cloud administrations are considered to be the complete collection for one's business[4].

2.2 Oracle Cloud Technologies

Oracle gives the complete enterprise read open cloud solutions, including IaaS, PaaS and SaaS. Users need to focus on their business with no concern about IT management. Oracle provides Oracle mobile cloud, Oracle cloud compute, Oracle cloud messaging and Database-as-a-Service[4].

2.3 Google Cloud Technologies

Google cloud also offers the services like SaaS, PaaS and IaaS. Google cloud empowers designers to manufacture, test and send applications on Google's highly extensible and secure framework. As we realize that Google has as of now given framework that permits Google to show huge hunt results in very short time, gives storage to around 425 million Gmail clients. Google can manufacture, sort out and work an enormous system of servers and fiber-optic cables .All this in total makes Google, the King of all cloud [4].

3. Security Architecture of Cloud Computing

Cloud security is particularly a troubling issue on account of the way that the devices are used to give services which don't have a place with the clients themselves. The clients have no control of, nor any information of, what could happen to their information. This creates a trouble in situations when clients have important and individual data put away in a cloud computing service. Clients won't trade off their security; providers must guarantee the protection of client's data.

SLA Monitor, Load Balancer, Advance Resource Reservation Monitor, Accounting, Resource Provisioning, Scheduler& Dispatcher, Metering and Policy Management are the significant segments of Service Provider Layer. A portion of the issues of security identified with Service Provider Layer are People and Identity, Binding Issues, Identity, Audit and Compliance, Infrastructure, Privacy, Data transmission and Cloud integrity.

Virtual Machine Layer creates and monitors number of VMs and number of operating systems and its monitoring. A portion of the issues of security identified with Virtual Machine Layer are VM Sprawl, VM Escape, Infrastructure, Separation between Customers, Cloud legal and Regularity issues, Identity and Access management. Significant segments of Data Centre (Infrastructure) Layer are the Servers, CPU's, networks and storage. A portion of the issues of security identified with Data Centre Layer are secure data at rest, Physical Security: Network and Server.

A few organizations or associations concentrating on issues of security in cloud computing, namely, Cloud Security Alliance (CSA), Open Security Architecture(OSA), etc.,. Figure 1 presents the high level outlook of security architecture of cloud computing, consists of four levels such as security authentication, data transmission security, virtual machine security and server /network/data storage security[5].

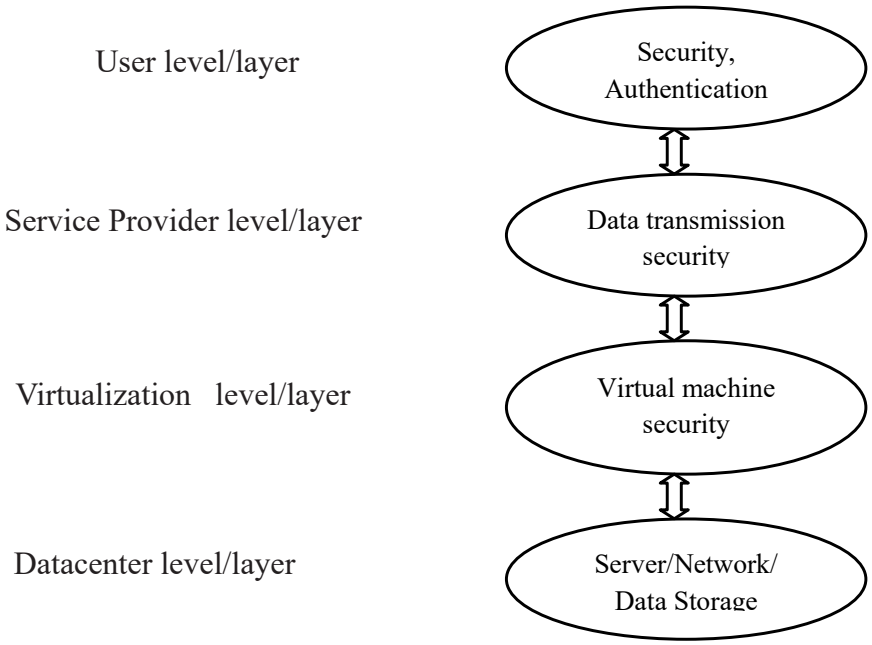

Figure 1. High level security architecture of cloud computing.

4. Security Issues in Delivery Models

Cloud computing comprises of packages, platforms and framework components. Each issue plays diverse activities and offers one-of-a-kind products for organizations. In cloud computing, three popular delivery models namely SaaS, PaaS, and IaaS, delivers services to the end users. These models have distinctive levels of security requirements[6].

4.1 Security Issues in SaaS

In SaaS model, service provider facilitates the software applications and accessible by clients on requests, over the web. SaaS is a model, where customer information is accessible and transparent to different clients over the internet. To protect data, an obligation of service provider is to frame appropriate security checks. It is a significant security issue in storage and secure migration of data.

The consecutive measures ought to be checked in SaaS application change process such that Data Security, Data locality, Data integrity, Data separation, Data access, Data confidentiality, Data breaches, Network Security, Authentication and authorization, Web application security, Identity management process[2].

Some of the essentials issues through which malicious client get to access and abuse the data security, store at the SaaS merchant such that SQL Injection flaw, Cross-site request forgery, Insecure storage and configuration, and Cross-site scripting.

4.2 Security Issues in PaaS

PaaS manages operating system, middleware, and so forth and resides on top of IaaS. PaaS provides complete platform and the place where with no delay user performs development task. The service provider provides few commands to client across some application on platform. Yet at the same time there is a security issue such as intrusion and so on, should guaranteed that data is not open among applications.

4.3 Security Issues in IaaS

This layer offers fundamental security firewall, load balancing, and so on. In IaaS, security is provided and no gap in the VM. Trustworthiness of data is a fundamental issue of security in IaaS.

To deliver the difficulties furthermore to empower cloud computing, some of the test bed groups, namely, CSA, Internet Engineering Task Force (IETF), Storage Networking Industry Association (SNIA) so on, are creating specifications and takes consideration of already available standards.

5. Types of Clouds

There are four types of clouds relying upon infrastructure ownership. Each cloud contains merits and demerits. This is the place where issues regarding security starts[7].

5.1 Public Cloud

This is available for open use and for large industry group, managed by service provider. Less secure than private clouds. Example: Google's Gmail or Drop box, Sun Cloud, Amazon AWS, Microsoft BPOS, IBM's Blue Cloud, Google Applied Engineering, Microsoft Office 365, Salesforce.com and Windows Azure Services Platform.

Public cloud benefits are:

i. Easy to use and no upfront commitments.
ii. Scalability.
iii. No wastage of resources, open cloud works on pay-per-use basis.

5.2 Private Cloud

It is functioned exclusively for use of an organization. Organization itself controls and manages Personal Cloud. It may either be on or off premises. Example: Amazon's EC2 or S3.

Benefits of using private cloud are:

i. To maintain confidentiality in highly sensitive electronic records.
ii. It is highly secured deployment model

5.3 Hybrid Cloud

It is nothing but multiple clouds combination, namely private, public and community, where each cloud has unique identities. It also provides application portability. Example**:** Force.com and Microsoft Azure, Health care, trade…etc;

Benefits of using a hybrid cloud service are:

i. It enables organizations to defend their information and programs on a personal cloud and reduce IT operational fees with the aid of storing the shared data on the open cloud.
ii. To interact with users use Public cloud and provide security to their data using Private cloud.

5.4 Community Cloud

Its one where cloud has been organized to serve common purpose or function managed by constituent organizations or by third party.Table1 shows the different cloud

Table 1. Cloud deployment models and issues

Model	Public	Private	Hybrid
Security issues	i)Least secure ii)Multi-tenancy iii)Transfers over the net	Most secure	Control of security between Private and Public clouds

Table 1 Continued

Cost issues	i)Setup: High ii)Usage: lowest (pay for what you use)	i)Setup: High ii)New operational processes are required	--
Control issues	Least control	Most control	Least control
Legal issues	Jurisdiction of storage	--	Jurisdiction of storage

deployment models and various issues[7–8]. The most secure and controlled deployment model is private cloud.

6. Cloud Computing Security Issues

6.1 Network Transport Security

In networks, Network transport security concerns about data transmission security, to guarantee that the data won't be caught, altered, or replaced in this procedure.

The cloud network topics are: DNS attack, Reused IP address, Sniffer attack, Man in the middle attack, Denial and distributed denial of Service attack, etc[9].

At present, Internet uses open protocols and depends on protocols like TCP / TP , its datagram formats, so while doing transmission effortlessly data can be blocked, plaintext secret word i.e., password, are even utilized by some applications. Secure transmission protocol (SSL) is an encryption protocols possess the better capacity to provide data transmission security. Service providers give more noteworthy security to customers and their exceptional encryption and also provision of authorized certification center from others. Network security equipment and modern cryptographic algorithms are coupled Hypertext Transfer Protocol (HTTPS) or Transmission Control Protocol (TCP) / Transaction Processing (TP) protocols to ensure the secure data transmission in on the network[10].

6.2 Data Storage Security

It is nothing but ensuring the data security on the storage media, in case of data loss, it ensures fast restorable and non volatile. While designing cloud storage services by software engineers, security measures ought to be considered. Data replication, isolation and dynamic are included in data storage security. Essential measures of storage media to ensure data security is data redundancy , and dynamic implies frequent changes of client data, so need some measures to guarantee consistency of data. Isolation avoids dependencies between data and data changes by different clients won't influence the present client[10].

6.3 Cloud Confidentiality

In cloud environments, confidentiality infers that cloud provider and other customers are unaware of client's information and computation assignments. Confidentiality stays as extreme concern in cloud computing. This is to a great extent owing to the way that untrustworthy cloud providers controls and manages cloud servers where client's information and computation assignments are stored[11].

Some of the Threats to Cloud Confidentiality are[11]

6.3.1 Cross-VM Attack via Side Channels[12]

Multi-tenancy nature of cloud computing misuses by the attack, called cross-VM attack, empowers that same physical machine can hold VMs belongs to distinct cli-

ent's. Insidious threat such as regard timing side-channels to cloud security owing to that a) difficult to control the gigantic parallelism nature and shared infrastructure and existence of timing channels; b) without raising alarms malicious customers are in a position to copy others information. Steps to initiate this attack are placement and extraction[13].

6.3.2 Malicious SysAdmin

Cloud provider privileged sysadmin can attack by getting into the client's VMs memory. Example, Xenaccess[14] empowers a sysadmin to get to the memory of VM run time by executing procedure at client level in Domain.

Existing Strategy to avoid cross-VM attack is of six categories[11]

i) reduces the success rate of placement by means of placement prevention; ii) physical isolation implementation iii) fresh cache designs; iv) by eliminating fine-grained timers fuzzy time means to exhaust malicious VM's capability of receiving the signal; v) leakage of non-deterministic information of others to adversaries; vi) cryptographic implementation of timing-resistant cache.

6.4 Cloud Integrity

Like confidentiality, in cloud computing the idea of integrity deal with two types of integrity: data integrity and computation integrity. The former suggests that identification of damages such as data loss, modification of data, etc., and genuine storage of data on cloud servers. The latter suggests that identification of wrong computations and the thought that without being mutilated by other malicious clients or malware, programs are executed[11].

Some of the threats to Cloud Integrity are[11]:

6.4.1 Data Loss/Manipulation

Data of the clients get stored on remote data centres, data is not under the control of their owners, and attackers may take advantage of this to initiate attack. Data loss may also create by administration errors such as uphold and recondition, migration of data, and dynamic memberships in P2P systems.

6.4.2 Dishonest Computation in Remote Servers

Cloud customers are unaware of computation details, cloud servers might act trust less and answer wrong consequences, might not take after the semi-open model. Even semi-open model is followed some issues might emerge, when a cloud server contains before attacked malicious code or data and utilizes past, unprotected code.

Existing strategies of checking data integrity in cloud are[11]: Provable Data Possession (PDP), Scalable PDP, Dynamic PDP, High-Availability and Integrity Layer (HAIL), Third Party Auditor, Combating dishonest computing.

6.5 Cloud Availability

On-demand self service of various levels is the basic feature of cloud computing, hence availability is vital. Clients might not have confidence in the cloud system in case of no more service accessible or its quality doesn't fit SLA (Service Level Agreement).

Some of the threats to Cloud Availability are[11]

6.5.1 Flooding Attack via Bandwidth Starvation

Two types of these attacks are

- *Direct DOS* – first target cloud is resolved, and then attack target cloud and its services will be no longer accessible.
- *Indirect DOS* – two phases of Indirect DOS is: 1) influences physical machine services available with the objective victim; 2) without determining a particular target, the attack is started.

6.5.2 Fraudulent Resource Consumption (FRC) Attack

The aim of attack is to deny the normal customers of their long-term financial accessibility of facilitating freely open contents of web. Attackers utilize bandwidth by persistently sending requests to the website and acts as legal clients, bills given to the owners of the website (client).

Existing approaches of cloud availability in cloud computing are[11]: Defending the new DOS attack and FRC (Fraudulent Resource Consumption) attack detection.

6.6 Cloud Accountability

In cloud computing, multiple parties might be included, the essential ones among them are cloud provider and its customers. To recognize a particular machine or flawed program that is mindful, identity might be utilized.

Some of the threats to Cloud Accountability are[11]

6.6.1 SLA Violation

The problems that may emerge : 1) degenerate the client's information or alternately dispute calculations that gives wrong output in the cloud owing to the misconfigured or alternately damaged machines; 2) client's services performance might be degraded by the allocation of insufficient resources by cloud provider for the client and break the SLA; 3) In order to create Dos assaults or spamming on clients machines, in request to take sensitive information or to attain control over clients machine, an attacker installs bugs into the software of client; 4)data unavailable and the client might not access to their information.

6.6.2 ishonest MapReduce

In MapReduce a huge data set is divided into numerous blocks, for processing single worker machine are assigned individual input for processing. Malicious or misconfigured working machines, subsequently, returns inaccurate results after processing. Also, it is not easy for client's to confirm the rightness of results. Example for computation integrity problem is Dishonest MapReduce. Even after client's verification on output correctness, yet try to recognize faulty machines that give inaccurate output, so this issue will be further tended by accountability.

Existing approaches of cloud accountability in cloud computing are: Accountability on SLA, Accountable MapReduce.

6.7 Cloud Privacy

Usually the data are distributed worldwide in clouds. Worries about data exposure, legal power and privacy hikes owing to data distribution. In fact, the cloud provider possessed and asserted cloud servers where business logic and data of clients get stored and distributed among cloud servers. Hence, privacy is yet another crucial issue in cloud computing[11].

Some of the threats to cloud privacy are[11]

6.7.1 Privacy-preservability

It is a rigid confidentiality form, because both prevent data leakage. Privacy-preservability will be damaged, if confidentiality is abused. Cloud privacy is nothing but a collection of data privacy and computation privacy.

Existing approaches of cloud privacy in cloud computing are[7]: Full Homomorphic Encryption (FHE), Privacy manager that relies on obfuscation techniques, there is an architecture that offers different privacy levels to customers rendered as Three-level protection of data architecture and so on.

7. Conclusion

In this paper, we have spotlighted some of the issues of cloud security. It is hard to arrive at an end-to-end security owing to the cloud complications. Setting up of fresh strategies of security has to be answered and more established procedures regarding security should have been fundamentally changed to have the capacity to work with the cloud architecture.

8. References

1. Hwang K, Geoffrey C, Fox G, Dongarra JJ. Distributed and cloud computing from parallel processing to the Internet of things (ed.). Software Engineering and Programming; 2011. p. 672.
2. Kondo D, Javadi B, Malecot P, Cappello F, Anderson DP. B Cost-benefit analysis of cloud computing versus desktop grids, In: Proceedings of IEEE International Symposium on Parallel and Distributed Processing, Rome, Italy; 2009. p. 1–12.
3. Ostermann S, Iosup A, Yigitbasi N, Prodan R, Fahringer T, Epema D. A performance analysis of EC2 cloud computing services for scientific computing, In: Cloud Computing, Springer Berlin Heidelberg. 2010; 34:115–31.
4. Sharma R, Kes TR. Literature review: cloud computing – security issues, solution and technologies. International Journal of Engineering Research. 2014; 3(4):221–5.
5. Padhy RP, Patra MR, Satapathy SC. Cloud computing: security issues and research challenges. International

Journal of Computer Science and Information Technology and Security. 2011; 1(2):136–46.
6. Khan AW, Khan SU, Ilyas M, Azeem MI. A literature survey on data privacy/ protection issues and challenges in cloud computing. IOSR Journal of Computer Engineering. 2012; 1(3):28–36.
7. Balasubramanian R, Aramudhan M. Security issues: public vs. private vs. hybrid cloud computing. International Journal of Computer Applications. 2012; 55(13):35–41.
8. Cloud computing mini-guide [Internet]. 2016 [cited 2016]. Available from: http://searchcloudcomputing.techtarget.com/tutorial/Cloud-computing-mini-guide.
9. Beulah S, Dhanaseelan FR. Survey on security issues and existing solutions in cloud storage. Indian Journal of Science and Technology. 2016; 9(13):1–8.
10. Meng D. Data security in cloud computing, The 8th International Conference on Computer Science & Education Colombo, Sri Lanka; 2013.
11. Xiao Z, Xiao Y. Security and privacy in cloud computing. IEEE communications surveys and tutorials, second quarter. 2013; 15(2):843–59.
12. Ristenpart T, Tromer E, Shacham H, Savage S. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds, Proceeding of 16th ACM conference on Computer and communications security, USA; 2009. p. 199–212.
13. Aviram A, Hu S, Ford B, Gummadi R. Determinating timing channels in compute clouds, In Proceeding of ACM workshop on Cloud computing security workshop ACM, New York, NY, USA; 2010. p. 103–8.
14. Payne BD, Carbone M, Lee W. Secure and flexible monitoring of virtual machines, In 23rd Annual, Computer Security Applications Conference on Atlanta; 2007. p. 1–13.