Cloud Computing Security Challenges: A Review

Iqra Kanwal, Hina Shafi, Shahzad Memon, and Mahmood Hussain Shah

Abstract Over the last two decades, cloud computing has gained tremendous popularity because of ever growing requirements. Organizations that are heading towards cloud-based data storage options have several benefits. These include streamlined IT infrastructure and management, remote access with a secure internet link from all over the globe, and the cost-effectiveness that cloud computing can offer. The related cloud protection and privacy issues need to be further clarified. This paper aims to discuss all possible issues that are under research and are resisting consumers to migrate from traditional IT environment to new trend of cloud computing which offers flexible and scalable environment at low-cost.

Keywords Cloud computing · Security · Confidentiality · Research challenges · Cloud security

1 Introduction

According to some researchers Cloud Computing is not completely a new technology, its roots somehow lies under "Computing as a Utility" and "Grid computing" [1, 2]. Others differ from this view and according to them it is totally independent computing [3]. At the higher level of this discussion. Cloud Computing is revolutionizing the way of computing. The vision of cloud computing is not to buy either hardware or

I. Kanwal · H. Shafi · S. Memon
Faculty of Engineering and Technology, University of Sindh, Jamshoro, Pakistan
e-mail: iqra.lakho@usindh.edu.pk

H. Shafi
e-mail: hunnyshafi@gmail.com

S. Memon
e-mail: shahzad.memon@usindh.edu.pk

M. H. Shah (✉)
Northumbria University, Newcastle upon Tyne, UK
e-mail: mahmood.shah@northumbria.ac.uk

H. Jahankhani et al. (eds.), *Cybersecurity, Privacy and Freedom Protection in the Connected World*, Advanced Sciences and Technologies for Security Applications, https://doi.org/10.1007/978-3-030-68534-8_29

even software instead rent services e.g. computational power, databases, storage, and other resource one just requires a vendor for that according to pay-as-you-go model, it reduces cost and makes investment oriented to operations rather than to assets acquisition. It refers to provision of hosted services over the Internet that are scalable and dynamic. Consumers can access the services online from their web browser without knowing the underlying technical details and difficulties of the resources.

Many researchers have given various definitions but one definition by National Institute of Standards and Technology (NIST) is that "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models" is most accepted one [4].

1.1 Cloud Service Delivery Models

As the NIST definition suggests, cloud based system provides its clients with on-demand services and these can be regarded as service models which include software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). Table 1 shows the main features of each service model, theirs users, infrastructure management, and some of the applications of these models.

Software as a Service (SaaS) It enables the customer to utilize applications running on the provider's server machine that is a cloud. Several clients can access these applications by using an interface that is a web browser, they consume the services on pay-as-you-go license subscription that significantly decreases the investment cost. SaaS is mostly used to implement business software applications at minimum charges.

Platform as a Service (PaaS) PaaS a group of software development programs and tools that are hosted on the cloud infrastructure. It is a service offered to developers which provides all the tools needed for system development. Client does not need to manage or administer computing hardware or software.

Infrastructure as a Service (IaaS) Resources can be rented as pay-per-use such resources can be storage, processing, network capacity and other computing facilities can be granted. Client can also have privilege to manage operating system and other applications. This model provides a flexibility to add or release resources and services upon requirement.

Table 1 Cloud service models

Delivery model	SaaS	PaaS	IaaS
Features	Provide software applications, used by consumers running on cloud infrastructure Examples include Software distribution model, collaboration, business processes, CRM/ERP/HR	Providing a framework for the creation, implementation and management of cloud computing solutions Examples include Web 2.0 Application, Middle-ware, Java Runtime, Tools for Development, Database	Provide hardware resources e.g. network, storage, memory, processor etc. as a virtual systems which are accessed by using Internet. Examples include servers, Networking, Data Center Fabric, Storage etc.
User	End client/End User Person or organization that subscribes a service	Developr-moderator An organization or a person that develops or deploys cloud	An organization or a person who owns cloud deployed infrastructure
Infrastructure management	Controlled by SaaS Provider	PaaS user control deployment of their individual applications and does not manage servers and storage	Controlled IaaS Provider Client is capable to launch virtual machines with any required operating systems that are managed by the clients
Applications	Google Apps (Gmail, Docs.) Salesforce CRM	Google App Engine Microsoft Azure Manjrasoft Aneka	Amazon EC2, S3 OpenNebula

1.2 Cloud Deployment Models

In literature five cloud deployment models have been discussed so far. These are public, private, hybrid, community and virtual private cloud (VPC). Among these models VPC has got less consideration by the research community [5]. Characteristics of these deployment models are summarized in Table 2.

Public Cloud In this cloud infrastructure is offered to the public on commercial basis which is own by an organization that is providing cloud services. People can rent resources and can scale up or down their utilization as desired.

Private Cloud In this model cloud infrastructure is dedicated and private system to an organization. It can be owned or rented by the organization. This may be managed by third party or organization itself.

Community Cloud This model is for the organizations having similar concerns and requirements. Cloud infrastructure is shared among more than one companies on shared cost. It is managed by the companies or a third party, located either within or outside the premises.

Hybrid Cloud Hybrid cloud is mash of multiple clouds (public, private, community), but managed and provided as a single unit by provider. The idea to use hybrid cloud mainly provide additional resources on user demand, e.g. an organization may

Table 2 Cloud deployment model characteristics

Deployment model	Characteristics
Public Cloud	Offered publically on commercial basis People rent the resources with the ability to scale them Cloud Service Provider (CSP) is responsible to own and manage a public cloud Located off-premises to the consumers Less secure than other cloud models
Private Cloud	Dedicated infrastructure for an organization for its private use Owned or rented by the organization Located either on- premises or off-premises Managed within the organization or externally More safe than the cloud that is public
Community Cloud	Shared with organizations that have similar concerns and requirements Located either on or off-premises Run by the businesses or externally
Hybrid Cloud	Mash of two or more clouds, provided as a single unit by provider Used to provide additional resources in case of demand Require both on and off-premises resources
Virtual Private Cloud	Private cloud, deployed on top of the any above mentioned cloud models over Virtual Private Network (VPN) Provide isolated resources to its consumers Characteristics are inherited by underlying cloud architectures upon which a VPC is seated

want to migrate some jobs from a private cloud to public, for this migration a hybrid cloud can be a choice.

Virtual Private Cloud (VPC) VPC is a private cloud, deployed on any above mentioned cloud models using Virtual Private Network (VPN). Its example is Amazon VPC [6]. In VPCs private and semi-private clouds are provided to the customers by VPN that provide isolated resources to its consumers. Since it is less discussed among research community, its cost, management, tenants and other characteristics are inherited from the underlying cloud models on which a VPC is seated up [5].

2 Cloud Computing Security Challenges

Although a lot of challenges are faced by emerging cloud computing technology such as interoperability, scalability, Service Level Agreement (SLA), lack of standards, continuously evolving, compliance concerns etc., security is major barrier into the adoption of cloud computing technology. Manage and maintain secure cloud computing environment is more difficult task than traditional information technology (IT) environment. As the cloud computing environment is an outsourcing of IT, along with the inherited security issues of IT environment, cloud computing also

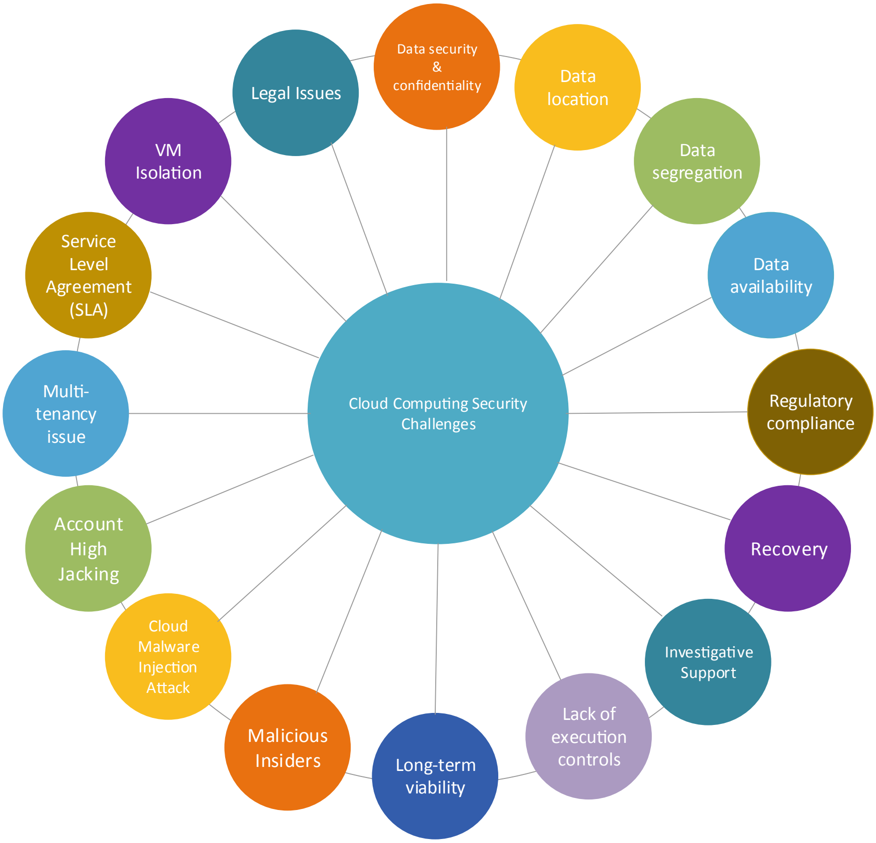

Fig. 1 Cloud computing security challenges

come across with some additional security challenges that are focused by researcher community in the last two decades which are highlighted here [3, 5, 7–27]. These security challenges are summarised in Fig. 1.

2.1 Data Security and Confidentiality Issues

Cloud consumer need to make sure their technology save cost and never sacrifice valuable data because there are several ways of data being compromised. The amount of risk increases due to the way in which a cloud particularly increases, due to which it may demand to remove and modify record, if the encoding key is lost it's also much painful. Some of them are unique due to the nature of cloud and complex too to recover because of cloud architecture [28]. CSA's suggested solutions include strong access control API implementation, data integrity and encryption and its protection while data transfer, implementing generation of strong key, analyzing the data protection at design and also at run time. While considering security of cloud computing the data comes at top most priority. Data theft and corrupted storage are two major risks in data protection.

2.2 Data Location

One of the issues of security and confidentiality (i.e. user location, relocation of user data and services, availability and security etc.) is data location. SaaS users use these applications for the processing the business data. Users of these services have no information of the location where their data is being kept. It can be challenging in many ways, since data security and compliance rules in different states the data location is of utter important in several enterprise architecture. For instance in various South America and European countries there is some types of data that cannot cross the border due to confidentiality reasons. Besides this issue of local rules and law, when an investigation takes place, it raises a question that the data falls at which jurisdiction. SaaS service model must also provide assurance of the location of the user data.

2.3 Data Segregation

Due to multitenancy, multiple users are capable to store use the data using SaaS services. In these situations the data of multiple users is stored on same location. Data intrusion is a threat in this condition. Attackers can inject their code into the SaaS service to hijack the system. It is possible that clients may run that code accidently without proper verification which leads high potential risk to other client's data. It is obligation to SaaS application to guarantee boundary between each client data. It is also required to maintain this boundary at physical as well as at service level and an application must segregate the data from different clients.

2.4 Data Availability

It is essential for SaaS cloud applications to guaranty twenty-four-seven services to their consumers. In order to provide high-availability and scalability, it is required to take measures at both design and architectural levels. Adaption of multi-tier architecture and support for application load balancing on various servers is needed. Recovery from hardware or software crashes, and denial of service attack must be built from within the service. Simultaneously, an action plan is needs for business continuation and disaster management for future crises. It is utterly important to offer safety measures to the organizations, minimal downtime, and maximum data availability.

2.5 Regulatory Compliance

Eventually, it is the consumer who is responsible to protect their data and data integrity even though if it's on the cloud. External audits and compliance certifications are carried out on conventional service providers. Providers of cloud computing who fail to conduct the scrutiny are "signaling that clients should only use them for the most trivial functions," Gartner says.

2.6 Recovery

Data recovery is very issue concern in cloud security when considering cloud data backup. Many cloud services moves data up to 5 TB within the 12 h. However certain systems may become slower because it all depends on storage speed, the amount of time to consider, and available storage in the server that is determining and negotiating this price. Backup availability in order to keep business running is very important. Data must be backed up during the recovery process.

2.7 Investigative Support

Any conceivable object, such as processing units, storage devices or applications, is distributed as services of cloud computing. The offered services are cost-effective and expandable. Enticing benefits from cloud computing draw tremendous interest from both company owners and cyber robberies. The "computer forensic inquiry" then take measures to find evidence against criminals. As a consequence of the new technologies and approaches that are being used in cloud computing, when examining the case, forensic investigative methods come across with various types of problems. These are difficult problems to cope with multiple decisions on the variety of data stored on many servers on various locations, restricted access to cloud evidence and also the problem of seizing physical evidence for the sake of validation of credibility or presentation of evidence.

2.8 Lack of Execution Controls

A user in a cloud system requires fine-grained access control of remote execution environment which the system lacks. Therefore, memory management, access to external utilities, I/O operations, and data are some of the crucial issues which are outside the purview of the user. In many scenarios the clients require to inspect execution to make sure that no illegal operations are performed but lack of execution control restricts from it.

2.9 Long-Term Viability

In an ideal situation a well-known cloud corporation will not split or be acquired by any other organization because it is very rear. But one must be sure of data availability if such condition occur. According to Gartner “Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application”.

2.10 Malicious Insiders

Rocha et al. [29] explained ways malicious insiders are able get unauthorized access to confidential information. They have provided a demonstration of some of attacks along with videos. They showed how easily some insider can get access to cryptographic keys, passwords, and other files. It often happens that the employees are provided with restricted amount of access to the system based on company policy but with high access, it is possible for them to get sensitive and restricted data and services. CSA enforces strict check on supply chain management, transparency in information management and security practices, reporting, specification of HR requirements as part of SLA, and defining security breach notifying procedures.

2.11 Cloud Malware Injection Attack

An attacker makes an attempt to inject malicious service or virtual machines into the cloud. In such attack, the attacker uses his malicious service module (PaaS or SaaS) or an instance of virtual machine (IaaS) and tries to augment the cloud system with it.

2.12 Account High Jacking

When all authentication practices are required, the account credential details between customers/users and services and the implementation of austere authentication techniques, organizations must get as minimal details as possible to locate their users' authentication problems individually. A key role in the user authentication process should not be played by the majority of publicly accessible information. It can be inferred that, regardless of design, an Incident Response Plan is of utmost importance.

There are different ways through which attackers use to accesses cloud accounts. Some of these are the use of reused passwords, which they try to different customers account until they open them.

2.13 Issue of Multi-tenancy

Multitenancy presents a problem for the users who run their services on same physical servers. The issue is to protect user data against data theft and unauthorized access from other users. This is also a concern of current web-hosting services. This dilemma needs to be seriously reexamined with the prevalent use of cloud computing because users store their substantial data on the cloud which require proper measures of security [30].

2.14 Service-Level Agreement

Service Level Agreements (SLAs) which define minimum output standards can be anticipated by the customer, e.g. 99.99% system availability in a year. Conventionally, however, security features such as privacy and confidentiality have not been considered by SLAs. Bernsmed [31] explained how SLA of a cloud which could be expanded in order to add some security aspects that allow multiple service providers given security levels to compose cloud services.

2.15 Virtual Machine (VM) Isolation

Virtual machines running on same hardware must be separated from each other. Although logical separation is already there between VM, still physical separation need to be there since resources are shared among servers and it can lead to data leakage.

2.16 Legal Issues

Legal issues arise due to conflicting legal jurisdictions and when cloud service provider share resources in different geographical locations because sometimes different data is available in different locations with diverse digital regulations.

3 Conclusion

Traditional computing practices has evolved with time and transformed into a new trend such as cloud computing. Cloud computing provides cost-effective, innovative, flexible, and optimized computing models. It allows numerous benefits to the world of computing and sets modern trends of advance level IT. Although it offers computing as a cloud with a simple internet connection, there are numerus security challenges that are yet to be addressed. Security has always remained a major challenge in computing and IT. Along with inherent security challenges of traditional systems, cloud computing comes with additional some additional security threats, risks, and challenges. This paper presented security challenges that are focused by the research community and need to addressed to enhance security concerns of cloud computing.

References

1. Stanoevska-Slabeva K, Wozniak T, Ristol S (2010) Grid and cloud computing: a business perspective on technology and applications
2. Foster I, Zhao Y, Raicu I, Lu S (2008) Cloud computing and grid computing 360-degree compared. In: Grid computing environments workshop, GCE 2008
3. Shaikh FBF, Haider S (2011) Security threats in cloud computing. In: 2011 International conference on internet technology and secured transactions, no December, pp 214–219
4. Mell P, Grance T (2011) The NIST definition of cloud computing. In: Cloud computing and government: background, benefits, risks
5. Freire MM, Inácio PRM (2014) Security issues in cloud environments : a survey, pp 113–170
6. Chauhan S et al (2018) Amazon virtual private cloud (Amazon VPC) and networking fundamentals. In: AWS® certified advanced networking official study guide
7. Varghese B, Buyya R (2018) Next generation cloud computing: new trends and research directions. Future Gener Comput Syst 79(September):849–861
8. Birje MN, Challagidad PS, Goudar RH, Tapale MT (2017) Cloud computing review: concepts, technology, challenges and security. Int J Cloud Comput 6(1):32–57
9. Cloud computing security issues and challenges, no Jan 2011, 2015
10. Yang C, Huang Q, Li Z, Liu K, Hu F (2017) Big data and cloud computing: innovation opportunities and challenges. Int J Digit Earth 10(1):13–53
11. Khorshed T, Ali ABMS, Wasimi SA (2012) A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Gener Comput Syst 28(6):833–851
12. Computing C (2014) A survey of cryptographic based security algorithms, vol 8, no March, pp 1–17

13. Zhang Q, Cheng L, Boutaba R (2010) Cloud computing: state-of-the-art and research challenges. J Internet Serv Appl 1(1):7–18
14. Mehraeen E, Ghazisaeedi M, Farzi J, Mirshekari S (2016) Security challenges in healthcare cloud computing: a systematic review. Glob J Health Sci 9(3):157
15. Mogos G (2019) Cloud security. Crit Anal 17(3):51–54
16. Sahmim S, Gharsellaoui H (2017) Privacy and security in internet-based computing: cloud computing, internet of things, cloud of things: a review. Procedia Comput Sci 112:1516–1522
17. Li J, Zhang Y, Chen X, Xiang Y (2018) Secure attribute-based data sharing for resource-limited users in cloud computing. Comput Secur 72:1–12
18. Paper C, Science PC (2015) State-of-the-art survey on cloud computing security challenges, approaches and solutions state-of-the-art survey on cloud computing security challenges, approaches and solutions, no June
19. Hamlen K, Kantarcioglu M, Khan L, Thuraisingham B (2010) Security issues for cloud computing. Int J Inf Secur Priv 4(2):36–48
20. Khorshed MT, Ali ABMS, Wasimi SA (2012) A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Gener Comput Syst 28(6):833–851
21. Sengupta S, Kaulgud V, Sharma VS (2011) Cloud computing security—trends and research directions. In: Proceedings of the 2011 IEEE world congress on services, no 4, pp 524–531
22. Abdul-Jabbar SS, Aldujaili A, Mohammed SG, Saeed HS (2020) 西南交通大学学报 Integrity and security in cloud computing environment: a review 云计算环境中的完整性和安全性:回顾. J Southwest Jiaotong Univ 55(1):1–15
23. Subramanian N, Jeyaraj A (2018) Recent security challenges in cloud computing. Comput Electr Eng 71(July):28–42
24. Fatima S, Ahmad S (2019) An exhaustive review on security issues in cloud computing. KSII Trans Internet Inf Syst 13(6):3219–3237
25. Tabrizchi H, Kuchaki Rafsanjani M (2020) A survey on security challenges in cloud computing: issues, threats, and solutions. J Supercomput 24(June):133–141
26. Zissis D, Lekkas D (2012) Addressing cloud computing security issues. Future Gener Comput Syst 28(3):583–592
27. Chen D (2012) Data Security and privacy protection issues in cloud computing, no 973, pp 647–651
28. Cloud Security Alliance (2010) Top threats to cloud computing. Security
29. Rocha F, Correia M (2011) Lucy in the sky without diamonds: Stealing confidential data in the cloud. In: Proceedings of the international conference on dependable systems and networks
30. Rong C, Nguyen ST, Gilje M (2013) Beyond lightning: a survey on security challenges in cloud computing q. Comput Electr Eng 39(1):47–54
31. Bernsmed K, Jaatun MG, Undheim A (2011) Security in service level agreements for cloud computing. In: CLOSER 2011—Proceedings of the 1st international conference on cloud computing and services science