ISSN: 0976-3104
ISSUE: COMPUTER SCIENCE

ARTICLE

CLOUD COMPUTING SECURITY ISSUES

Shubhankar Solanki, Wasim Khan, Harshit Arora, Dr Anupriya Jain*
FCA Department, Manav Rachna International Institute of Research and Studies
Delhi Suraj Kund Road, Sector 43, Faridabad, Haryana 121004, INDIA

ABSTRACT

*Today, cloud computing is a trending way of computing in computer science. Cloud computing is a set of resources and services that are offered by the network or internet provided by the third-party, allowing sharing of resources and data among devices. It is broadly used in many organizations nowadays and becoming more sought after because it changed the way resources (IT) of an organization are utilized and managed. It provides lots of benefits such as simplicity and lower costs, scalable storage capacity, low maintenance, ease of use, backup and recovery, 24*7 availability, quality of service, automatic software integration, flexibility and reliability, easy access to information. While there is increasing use of cloud computing service in this new era, the security issues of the cloud computing are becoming challenging. Cloud computing must be more safe and secure to ensure the privacy of the users. This paper focuses on the most common security issues of using cloud and certain solutions to the security issues. Security is one of the most crucial aspect in cloud computing due to the sensitivity of user's data.*

KEY WORDS
Cloud Security, Service Models, Deployment models, Security Threats, Security Techniques

Received: 21 Mar 2019
Accepted: 14 May 2019
Published: 2 June 2019

***Corresponding Author**
Email:
anupriya.fca@mriu.edu.in
Tel.: +91 9911293897

INTRODUCTION

Cloud Computing is a service model that produce various services in the form of on-demand services, it is accessible worldwide to everyone, everywhere and every time, including cloud referring to the web. In simple, Cloud Computing is a mixture of a technology that provides the hosting as well as storage service on the Internet. Its main intention is to provide scalable and affordable on-demand computing structure with superior quality of service levels [1]. Various national and international corporations are working on it and offer cloud computing services but they have not properly visualized the implications of accessing, processing and storing the data in a distributed shared environment. Many cloud-based application developers are struggling to include security. In multiple cases, the cloud developers simply cannot provide real security with the currently affordable technological capabilities [2]. Cloud computing concept is easy to understand as it allows us to share the resources on a greater scale .Distributed networks which requires less cost and is location independent. Resources on the cloud can be used by the consumers and deployed by the vendors such as Snapdeal, Google, IBM, Salesforce, Zoho, Rackspace, Flipkart etc[3]. Cloud computing model allows distributing the required on-demand services for various IT Industries. Benefits of Cloud computing are multifaceted. The most important benefit is that the users don't need to buy the resource from a third party vendor; rather they use the resources and pays for it as a service thus cloud helps the users to save time and also money. It is not only used by international companies but today it's also used by Small and medium enterprises [4].

Cloud Computing architecture includes multiple cloud component which interacts with each other for various data which leads the user to access data on a faster rate. Cloud is mainly consists of front and the back end. Front end is the user side that is accessing the data, whereas the backend is the data storage device, server which makes the Cloud. Cloud computing is of three different categories viz, private cloud, public cloud and hybrid cloud. The private clouds are taken care by single organization and the public clouds are taken care on a larger scale. The Private clouds provide better security control and more flexibility than other cloud types. Hybrid clouds are the combination of Private clouds and Public Clouds that are used by various industries [5].

The benefits of cloud computing may be very appealing but nothing is perfect. Because the Cloud computing got many security issues especially on Data theft, Data loss and Privacy. This research paper lists the parameters that affect the security of the cloud, explores the cloud security issues and problems that the cloud computing service provider and also the cloud service customer face by such as loss of data, privacy, infected application and security issues [6].

The various Security issues of these systems and technologies are appropriate to cloud computing systems. For example, the network that interconnects the systems in a cloud computing has to be secured. Moreover, the virtualization paradigm in the cloud computing results the various security concerns. For example, mapping the virtual systems to the physical systems has to be carried out securely [7]. Data security includes encrypting the data as well as ensuring that the significant strategies are enforced for data sharing. Furthermore, the resource allocation and memory management algorithms has to be secured. Finally, data mining method may be applied to malware detection in cloud computing [8].

BACKGROUND REVIEW

Being the most trending technology of the age, the research is being done widely on Cloud Computing and especially on cloud security. In December 2008, Cloud Security Alliance (CSA) was formed with the aim to provide assured security within cloud computing environment. CSA launched "Security Guidance for

IIOAB JOURNAL
ISSN: 0976-3104

Critical Areas of Focus in Cloud Computing" as their initial product to help users get better insight about clouds and the security parameters [9]. The Cloud Computing Interoperability Group and the Multi-Agency Cloud Computing Forum have made lot of efforts to deliver efficient and effective controls to provide information security in Cloud environment Till date, many efforts have been made to find main security issues in cloud. It is described that privacy and the trust are the major security issues faced by the cloud computing. Security and privacy challenges to cloud computing are discussed in a detail which also addresses the security issue. It is claimed that cloud systems can't prosper without resolving security and privacy issues. A cloud computing framework and information asset classification model were proposed to help cloud users choosing different delivery services and models [2].

RELATED WORKS

The architecture of cloud composed of several service and deployment models.

Service Model

Software as a service (SaaS)

It is the top layer of cloud service model. The cloud service provider developed and hosts the software or application on the cloud infrastructure allowing the users to use it with various devices by using the thin client interface such as web browser. However the underlying cloud infrastructure, network, servers, operating systems or even individual application capabilities is not manageable by the users. It helps the users to save cost because licensing of the traditional packages is more expensive compared to the monthly fee for renting the application from cloud service [1].

Platform as a service (PaaS)

A middle layer of cloud service model that provides a software environment or platform for the users to design, develop, deploy and test their application without worrying about the underlying of the cloud infrastructure using the virtual servers of the cloud service provided. Therefore, the users can build their own applications running on the provider's infrastructure and they can have control over the deployed application they built [1].

Infrastructure as a Service (IaaS)

The user is allowed to rent the processing, storage and other fundamental computing resources to deploy and run arbitrary software which include operating system and applications .It provides basic storage and computing capabilities. It also has a data centre space that can help to handle workload [1].

Table 1. Comparisons of service model and examples

	SaaS Consume	PaaS Build	IaaS Host
Consumer	**End User**	**Application Owner**	**Application Owner**
Type of Service Provided	▪ Completed Applications	▪ Run Time scenario ▪ Cloud storage ▪ Integration, etc	▪ Cloud storage ▪ Visual server
Coverage at Service Level	▪ Application uptime ▪ Application performance	▪ Environment availability ▪ Environment performance ▪ No application coverage	▪ Virtual server availability ▪ Time to provision ▪ No platform or application coverage
Examples of Services Provided	▪ ▪ CRM ▪ E-mails ▪ Collaborative ▪ ERP	▪ Application development ▪ Decision support ▪ Web ▪ Streaming	▪ Caching ▪ Security ▪ Legacy ▪ System management

Deployment models

Public cloud

Third-party cloud provider owned a public cloud that is publicly accessible cloud environment. Any user can access it and they can store their data in the same cloud provided by the cloud service provider. The creation and on-going maintenance of the public cloud and its IT resources is managed by cloud service provider. In several scenarios the science of architectures explored in upcoming segments involve public clouds and the relationship between the producer and consumers of IT resources via public clouds [6].

Private Clouds

A private cloud is owned by a Single organization or users and it is not shared with the others. The user has physical control over the cloud infrastructure where everyone shares a common cloud infrastructure and it is more secure compared to the public cloud. The services provided by it is host services on private network that assist most corporate network and data administrators to become in-house service provider

IIOAB JOURNAL
ISSN: 0976-3104

efficiently. Same organization is technically both the cloud provider and cloud consumer in a private cloud [6].

Hybrid Clouds

A hybrid cloud is a cloud environment comprises of two or more different cloud deployment models. It is a combination of the public, the private or even the community cloud infrastructure which allows the transitive information exchange. It increases the flexibility of the cloud infrastructure where the users can implement the private cloud using the public cloud resources. For example, a cloud consumer may choose to deploy cloud services, process sensitive data to a private cloud and other, less sensitive cloud services to a public cloud. The result of this combination is a hybrid deployment model. Hybrid deployment architectures can be complex and challenging to create and maintain due to the potential disparity in cloud environments and the fact that management responsibilities are typically split between the private cloud provider and the public cloud provider organization[6].

Community cloud

The cloud infrastructure is shared among organizations that share the same concerns such as the mission, security requirement and policy. It may owned by more organization and it can exist on premises or even off-premises.

Each type of cloud model provides different level of control, flexibility and management. The users should choose the most suitable type of cloud computing model based on their own situation and their unique needs. This is very important since using inappropriate cloud model might cause the users to suffer for a great loss such as reduced organization efficiency and might suffer serious consequences like data breaches, data loss and corrupt data [6].

SECURITY ISSUES

Organization uses various cloud services as IaaS, PaaS, SaaS and the models like public, private, hybrid. These models and services have various cloud security issues. Each service model is associated with some issues. Security issues are considered in two views first in the view of service provider who insures that services provided by them should be secure and also manages the customer's identity management. Other view is customer view that ensures that service that they are using is securing enough [10].

Security issues

Data at rest is the major issues in cloud computing because users may store all their common, private, or even sensitive data in the cloud which can be accessed by anyone and anywhere. Data theft is a very common issue that are facing by the cloud service providers nowadays. Beside, some cloud service providers don't even provide their own server because of the cost effectiveness and flexibility [10]. There are also incidents like data loss which might be a serious problem for the users. For example, the server is suddenly shut down and causes data loss of the users. Furthermore, natural disaster might also cause data to be damaged or corrupted. Therefore, physical data location can be considered as one of the security issues in cloud computing [11].

Privacy issues

The cloud computing service provider must enforce their own policies to ensure the safety of the data stored by the users in their cloud model. The security of the data must be ensured and only the authorized person can maintain the cloud service model. The security of cloud computing should be done on the service provider side and also the user side. Cloud service provider should provide a good layer of security protection for the users where the users are not allowed to tamper with other user's data. The cloud computing is a good way to reduce the cost and provide more storage if and only if the security is ensured by both service provider and user [12]. The authors claimed that regulatory reform is essential to protect sensitive data in the cloud since one of the most challenging aspect in cloud computing is to ensure that the consumer have trust in privacy and security of their data [12].

Application issues

Monitoring and maintenance should be done by the cloud service provider frequently to ensure that the cloud is secure and not infected by the malicious code that have been uploaded to the cloud by the hackers or attackers with the purpose of stealing sensitive information or even damaging the information of certain users [14].

Threat Issues

There are lots of security issues regarding the cloud computing that have been widely used nowadays. There are top nine threat that pose severe danger to the cloud computing in year 2013 according to "The Notorious Nine: Cloud Computing Top Threat" by the Cloud Security Alliance (CSA). The top nine threat that have been mentioned in the white paper are:

IIOAB JOURNAL
ISSN: 0976-3104

Data Breaches

Data breaches are in all forms and have existed for years. Despite of new technology, Cloud computing and services still have data breaches. A study conducted by the Ponemon Institute entitled "Man in Cloud Attack" reports that over 50 percent of the IT and security professionals surveyed believed their organization's security measures to protect data on cloud services are low. This study used nine scenarios, where a data breach had occurred, to determine if that belief is a fact. After assessing each scenario, the report concluded that overall data breaches was three times more likely to occur for businesses that make use of the cloud than those that don't. The simple conclusion is that the cloud comes with a exclusive set of characteristics that make it more vulnerable [14].

Hijacking of Accounts

The growth and implementation of the cloud in many organizations has opened a whole new set of issues in account hijacking. Now attackers have the ability to use your login information to access your sensitive data stored on the cloud; besides, attackers can alter information through hijacked credentials. Scripting bugs and reused passwords are other method of hijacking, which leads attackers to easily and often steal credentials. Amazon faced a cross-site scripting bug that targeted customer credentials as well Phishing, key logging, and buffer overflow similar threats in April 2010 [13].

Insider Threat

An attack from inside your organization may seem impossible, but the insider threat does exist. Employees can use their authorized access to an organization's cloud based services to misuse information such as customer accounts, financial forms, and other sensitive information. And these insiders don't even need to have mischievous intentions. Imperva, inc., has published, "An inside Track on Insider Threats". A report that examines that the psychological, legal and technological strategy employed by leading organizations to reduce insider threats, a class of enterprise risk sustain by trusted person who has access to intellectual data, but uses that information outside of acceptable business requirements [15].

Malware Injection

Malware injection is a code, insert into cloud services that act as "valid instances" and run as SaaS to cloud servers. In cloud, Malware injection attacks an attacker to inject mischievous services or virtual machine into the cloud. To prevent cloud from malware injection attack we can merge the integrity with hardware. We can use hardware for integrity purpose because for an attacker it is difficult to interfere in the IaaS level [16].

Abuse of Cloud Services

The development of cloud-based services has made it possible for both small and enterprise-level organizations to host vast amounts of data easily. However, the cloud's outstanding storage capacity has also allowed both hackers and authorized users to easily host and spread malware, illegal software, and other digital properties. This practice affects both the cloud service provider and its customer [17].

For example: privileged users can directly or indirectly increase the security risks and as a result infringe upon the terms of use provided by the service provider. These risks include the sharing of pirated software, videos, music, or books, and can result in legal consequences in the forms of fines and settlements with the U.S. Copyright Law reaching up to $250,000. Depending on the damage, these fines can be even more cost prohibitive. You can reduce your exposure to risk by monitoring usage and setting guidelines for what your employees host in the cloud. Service providers and legal entities, such as CSA have defined what is abusive or inappropriate behavior along with methods of detecting such behaviors [17].

Insecure APIs

Application Programming Interfaces (API) gives user the opportunity to customize their cloud experience. But, APIs can be a threat to cloud security because of their very nature. Not only they give companies the ability to customize features of their cloud services to fit business needs, but they also authenticate, provide access, and effect encryption. APIs give programmers the tools to build their programs to integrate their applications with other job-critical software. Simple example of an API is YouTube, where developers have the ability to integrate YouTube videos into their sites or applications. The vulnerability of an API lies in the communication that takes place between applications. While this can help programmers and businesses, they also leave exploitable security risks [18].

Denial of Service Attacks

Denial of service (DOS attack) is cyber-attacks in which the offender seeks to make a machine or network source unavailable to its intended users by temporarily disrupting services of a host connected to the internet. DOS is typically accomplished by flooding the targeted machine or resources with superfluous requests in an attempt to overload systems and prevent some legitimate requests from being fulfilled. In some cases, however, DOS is also used as a smokescreen for other malicious activities, and to take down security appliances such as web application firewalls [11].

Insufficient Due Diligence

Most of the issues we've looked at here are technical in nature, but this particular security gap occurs when an organization does not have a clear plan for its goals, resources, and policies for the cloud. Insufficient due diligence- with cloud computing being a new implementation, especially to the hiring organizations, there is a knowledge gap that can prevent sufficient exercise of due diligence when hiring a

IIOAB JOURNAL
ISSN: 0976-3104

cloud service provider. In other words, it's the people factor. This is especially important to companies whose data falls under regulatory laws like PII, PCI, PHI, and FERPA or those that handle financial data for customers [13].

Shared Vulnerabilities

Cloud security is a shared responsibility between the service provider and the customer. This partnership between customer and provider requires the customer to take preventative actions to protect their data. While major providers like Box, Dropbox, Microsoft, and Google do have mass procedures to secure their side. As per article "Office 365 Security & Share Responsibility," the protection of user passwords, access restrictions to both files and devices, and multi-factor authentication – firmly in user hands. Hence the customers and service providers have shared responsibilities and omitting yours can result in your data being compromised [18].

Data Loss

Another serious threat is that an important data compromised due to deletion, modification, unlinking a record and storing of data on unreliable medium. It leads to loss of crucial data, reputation (for businesses), and trust of customers. Loss of data may cause severe legal and policy compliance issues. Malicious attack, natural disaster, or a data wipe by the service provider leads to a loss of data on cloud services. Losing important information can be devastating to businesses that don't have a recovery plan. In 2011 Amazon is an example of an organization that suffered data loss by permanently destroying many of its own customers' data [19].

TECHNIQUES TO SECURE DATA IN CLOUD

Authentication and Identity

Authentication of users and even of communicating systems is performed by various methods, but the most common is cryptography. Authentication of users takes place in various ways like in the form of passwords that is known individually, in the form of a security token, or in the form a measurable quantity like fingerprint. One problem with using traditional identity approaches in a cloud environment is faced when the enterprise uses multiple cloud service providers (CSPs). In such a use case, synchronizing identity information with the enterprise is not scalable. Other problems arise with traditional identity approaches when migrating infrastructure toward a cloud-based solution [20].

Data Encryption

If you are planning to store sensitive information on a large data store then you need to use data encryption techniques. Having passwords and firewalls is good, but people can bypass them to access your data. When data is encrypted it is in a form that cannot be read without an encryption key. The data is totally useless to the intruder. It is a technique of translation of data into secret code. If you want to read the encrypted data, you should have the secret key or password that is also called encryption key [20].

Information integrity and Privacy

Cloud computing provides information and resources to valid users. Resources can be accessed through web browsers and can also be accessed by malicious attackers. A convenient solution to the problem of information integrity is to provide mutual trust between service provider and user. Another solution can be providing proper authentication, authorization and accounting controls so that the process of accessing information should go through various multi levels of checking to ensure authorized use of resources. Some secured access mechanisms should be provided like RSA certificates, SSH based tunnels [20].

Availability of Information

Non-availability of information or data is a major issue regarding cloud computing services. Service Level agreement is used to provide the information about whether the network resources are available for users or not. It is a trust bond between consumer and service provider. A way to provide availability of resources is to have a backup plan for local resources as well as for most crucial information. This enables the user to have the information about the resources even after their unavailability [20].

Secure Information Management

It is a technique of information security for a collection of data into central repository. It is comprises of agents running on systems that are monitored and then sends information to a server that is called "Security Console". The security console is managed by admin who is a human being who reviews the information and takes actions in response to any alerts. As the cloud user base, dependency stack increase, the cloud security mechanisms to solve security issues also increase, this makes cloud security management much more complicated. It is also referred as a Log Management. Cloud providers also provide some security standards like PCI DSS, SAS 70. Information Security Management Maturity is another model of Information Security Management System [20].

Malware-injection attack solution

This solution creates a no. of client virtual machines and stores all of them in a central storage. It utilizes FAT (File Allocation Table) consisting of virtual operating systems. The application that is run by a client

ISSN: 0976-3104

can be found in FAT table. All the instances are managed and scheduled by Hypervisor. IDT (Interrupt Descriptor Table) is used for integrity checking [20].

CONCLUSIONS

Cloud computing is a promising and emerging technology for the next generation of IT applications. The barrier and hurdles toward the rapid growth of cloud computing are data security and privacy issues. Reducing data storage and processing cost is a mandatory requirement of any organization, while analysis of data and information is always the most important tasks in all the organizations for decision making. So no organizations will transfer their data or information to the cloud until the trust is built between the cloud service providers and consumers. A number of techniques have been proposed by researchers for data protection and to attain highest level of data security in the cloud. However, there are still many gaps to be filled by making these techniques more effective. More work is required in the area of cloud computing to make it acceptable by the cloud service consumers. This paper surveyed different techniques about data security and privacy, focusing on the data storage and use in the cloud, for data protection in the cloud computing environments to build trust between cloud service providers and consumers.

CONFLICT OF INTEREST

There is no conflict of interest.

ACKNOWLEDGEMENTS

This is to acknowledge to Dr. Pasenjit Bannerjee, Accendere Knowledge Management Services for his endless support for the successful completion of this paper. However, for any mistake the authors are solely responsible for that.

FINANCIAL DISCLOSURE

None.

REFERENCES

[1] Behl A. [2011] Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. 2011 World Congress on Information and Communication Technologies. IEEE, doi: 10.1109/WICT.2011.6141247.

[2] Behl A, Behl K. [2012] An analysis of cloud computing security issues. 2012 world congress on information and communication technologies. IEEE, doi: 10.1109/WICT.2012.6409059.

[3] Ertaul L, Singhal S, Saldamli G. [2010] Security Challenges in Cloud Computing. In Security and Management, doi: 10.1.1.722.4218.

[4] Mell P, Grance T. [2011]. The NIST definition of cloud computing. https://csrc.nist.gov/publications/detail/sp/800-145/final

[5] Mell P, Grance T. [2009] The NIST definition of cloud computing, version 15. National Institute of Standards and Technology (NIST). Information Technology Laboratory.

[6] Catteddu, D. [2009]. Cloud Computing: benefits, risks and recommendations for information security. In Iberic Web Application Security Conferenc). Springer, 10.1007/978-3-642-16120-9_9.

[7] Bhadauria R, Sanyal S. [2012] Survey on security issues in cloud computing and associated mitigation techniques. arXiv preprint arXiv:1204.0764.

[8] Jadeja Y, Modi K. [2012] cloud computing- concepts, architecture and challenges, IEEE, doi: 10.1109/ICCEET.2012.6203873.

[9] Balasubramanian R, Aramuthan DM. [2012]. Security problems and possible security approaches in cloud computing. Int J Sci Eng Res, 3(6), 1-4.

[10] Ukil A, Jana D, De S. [2013]. A security framework in cloud computing infrastructure. IJCSITS, 5(5), 11.

[11] Padhy RP, Patra MR, Satapathy SC. [2011]. Cloud computing: security issues and research challenges. IJCSITS, 1(2), 136-146.

[12] Dubey K, Kumar M, Chandra MA. [2015]. A priority based job scheduling algorithm using IBA and EASY algorithm for cloud metaschedular. In 2015 International Conference on Advances in Computer Engineering and Applications. IEEE, doi: 10.1109/ICACEA.2015.7164647.

[13] Srinivasan S, Raja K, Muthuselvan S. [2012]. Futuristic assimilation of cloud computing platforms and its services. In 2012 International Conference on Emerging Trends in Electrical Engineering and Energy Management (ICETEEEM). IEEE, doi: 10.1109/ICETEEEM.2012.6494467.

[14] Bakshi A, Dujodwala YB. [2010, February]. Securing cloud from DDOS attacks using intrusion detection system in virtual machine. In 2010 Second International Conference on Communication Software and Networks. IEEE, doi: 10.1109/ICCSN.2010.56.

[15] Bakshi A, Dujodwala YB. [2010, February]. Securing cloud from DDOS attacks using intrusion detection system in virtual machine. In 2010 Second International Conference on Communication Software and Networks. IEEE, doi: 10.1109/ICCSN.2010.56.

[16] Williamson A. [2011] Comparing cloud computing providers. Cloud Comp J, 2(3):3-5.

[17] Zhang X, Wuwong N, Li H, Zhang X. [2010] Information security risk management framework for the cloud computing environments. In 2010 10th IEEE international conference on computer and information technology. IEEE, doi:10.1109/CIT.2010.501.

[18] Reddy VK, Rao BT, Reddy LSS. [2011] Research issues in cloud computing. Global Journal of Computer Science and Technology, 11(11):59-64.

[19] Lim HC, et al. [2009] Automated control in cloud computing: challenges and opportunities. In Proceedings of the 1st workshop on Automated control for datacenters and clouds. doi:10.1145/1555271.1555275.

[20] Habib SM, Ries S, Muhlhauser M. [2010] Cloud computing landscape and research challenges regarding trust and reputation. In 2010 7th International Conference on Ubiquitous Intelligence & Computing and 7th International Conference on Autonomic and Trusted Computing, IEEE, doi: 10.1109/UIC-ATC.2010.48.