Data Security In Cloud Computing: A Review

Gurjeet Singh[1],Dr. Mohita Garg[2]

[1] Research Scholar, Department of Computer Engineering, NWIET, Moga

[2] Associate Professor, Department of Computer Science and Engineering, NWIET, Moga

mrgurjeet93@gmail.com , mohita_cse@northwest.ac.in

ABSTRACT

Cloud computing is Internet ("cloud") based development and use of computer technology ("computing"). It is a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet. Cloud computing uses the internet and the central remote servers to support different data and applications. It is an internet based technology. It permits the users to approach their personal files at any computer with internet access. The cloud computing flexibility is a function of the allocation of resources on authority's request. Cloud computing provides the act of uniting. Scientific computing in the 21st century has evolved from fixed to distributed work environment. The current trend of CloudComputing (CC) allows accessing business applications from anywhere just by connecting to the Internet. Evidence shows that, switching to CC organizations' annual expenditure and maintenance are being reduced to a greater extent. However, there are several challenges that come along with various benefits of cloud computing. Among these include securityaspects. Our aim is to identify security challenges for adapting cloud computing and their solutions from real world for the challenge that do not have any proper mitigation strategies identified. This non-existence of global standards and guidelines could be help academics to know the state of practice and formulatebetter methods/standards to provide secure interoperability. The identified cloud computing security challenges and solutions can be referred by practitioners to understand which areas of security need to be concentrated while adapting/migrating to a cloud computing environment.

KEYWORDS

Cloud computing, Virtual machine, Host, Datacenter, Datacenter Broker, Security

Language: English

Date of Publication: 30-07-2018

DOI: 10.24297/ijct.v17i2.7551

ISSN: 2277 - 3061

Volume: 17 Issue: 02

Journal: International Journal Of Computers & Technology

Website: https://cirworld.com

INTRODUCTION

Cloud could be a term used as a trope for the wide space networks (like internet) or several such giant networked atmosphere. It came partially from the cloud like image wont to represent the complexities of the networks within the schematic diagrams. It represents all the complexities of the network which can hold everything from cables, routers, servers, knowledge centers and every one such alternate device. Cloud computing is an on demand service in which shared resources, information, software and other devices are provided according to the clients requirement at specific time. It's a term which is generally used in case of Internet. The whole Internet can be viewed as a cloud. Capital and operational costs can be cut using cloud computing [36].With traditional desktop computing, we run copies of software programs on our personal computer. The documents we make are stored on our own pc. Although documents can be accessed from other computers on the network, they cannot be accessed by computers outside the network. This is PC-centric. By cloud computing, the software programs one use are not run from one's personal computer, but are quite stored on servers accessed via the Internet. If a computer crashes, the software is still available for others to use. Similar goes for the documents one create; they are stored on a collection of servers accessed through the Internet. Anyone with permission can not only access the documents, but can also edit and cooperate on those documents in real time.

Figure 1. Cloud Computing Model

BENEFITS OF CLOUD COMPUTING

Some common benefits of cloud computing are:

• **Reduced Cost:** Since cloud technology is implemented incrementally (step-by-step), it saves organizations total expenditure.

• **Increased Storage:** When compared to private computer systems, huge amounts of data can be stored than usual.

• **Flexibility:** Compared to traditional computing methods, cloud computing allows an entire organizational segment or portion of it to be outsourced.

• **Greater mobility**: Accessing information, whenever and wherever needed unlike traditional systems (storing data in personal computers and accessing only when near it).

• **Shift of IT focus:** Organizations can focus on innovation (i.e., implementing new products strategies in organization) rather than worrying about maintenance issues such as software updates or computing issues. These benefits of cloud computing draw lot of attention from Information and Technology Community (ITC). A survey by ITC in the year 2008, 2009 shows that many companies and individuals are noticing that CC is proving to be helpful when compared to traditional computing methods.

CLOUD COMPUTING: SERVICE MODELS

Cloud computing can be accessed through a set of services models. These services are designed to exhibit certain characteristics and to satisfy the organizational requirements. From this, a best suited service can be selected and customized for an organization's use. Some of the common distinctions in cloud computing services are Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Infrastructureas a Service (IaaS), Hardware-as-a-Service (HaaS) and Data storage-as-a-Service (DaaS). Service model details are as follows:

• **Software as a Service (SaaS)[4]**: The service provider in this context provides capability to use one or more applications running on a cloud infrastructure. These applications can be accessed from various thin client interfaces such as web browsers. A user for this service need not maintain, manage or control the underlying cloud infrastructure (i.e. network, operating systems, storage etc.). Examples for SaaS clouds are Salesforce, NetSuite.

• **Platform as a Service (PaaS)[5]**: The service provider in this context provides user resources to deploy onto cloud infrastructure, supported applications that are designed or acquired by user. A user using this service has control over deployed applications and application hosting environment, but has no control over infrastructure such as network, storage, servers, operating systems etc. Examples for PaaS clouds are Google App Engine, Microsoft Azure, Heroku.

• **Infrastructure as a Service (IaaS)**: The consumer is provided with power to control process, manage storage, network and other fundamental computing resources which are helpful to manage arbitrary software and this can include operating system and applications. By using this kind of service, user has control over operating system, storage, deployed applicationsand possible limited control over selected networking components. Examples for IaaS clouds are Eucalyptus (The Eucalyptus Opensource Cloud-computing System), Amazon EC2, Rackspace, Nimbus.

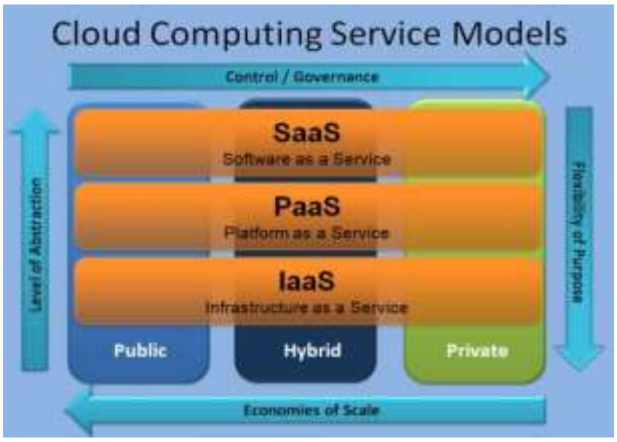

Figure 2. Service Models

CLOUD COMPUTING: DEPLOYMENT MODELS

Among the service models explained above, SaaS, PaaS and IaaS are popular among providers and users. These services can be deployed on one or more deployment models such as, public cloud, private cloud, community cloud and hybrid cloud to use features of cloud computing. Each of these deployment models are explained as follows:

• **Public cloud:** This type of infrastructure is made available to large industrial groups or public. These are maintained and owned by organization selling cloud services.

• **Private cloud:** This type of cloud deployment is just kept accessible to the organization that designs it. Private clouds can be managed by third party or the organization itself. In this scenario, cloud servers may or may not exist in the same place where the organization is located.

• **Hybrid cloud:**Within this deployment model there can be two or more clouds like private, public or a community. These constituting clouds (combinations of clouds used, such as `private and public', `public and community', etc.) remain different but yet bound together by standardized or preparatory technology that enables application and data portability.

• **Community cloud:** This type of cloud infrastructure is shared by several organizations and supports a specific community with shared concerns. This can be managed by an organization or third party and can be deployed off or in the organizational premise.

Usage of deployments models and services modeled provided by CC changes how systems are connected and work is done in an organization. It adds up dynamically expandable nature to the applications, platforms, infrastructure or any other resource that is ordered and used in CC.

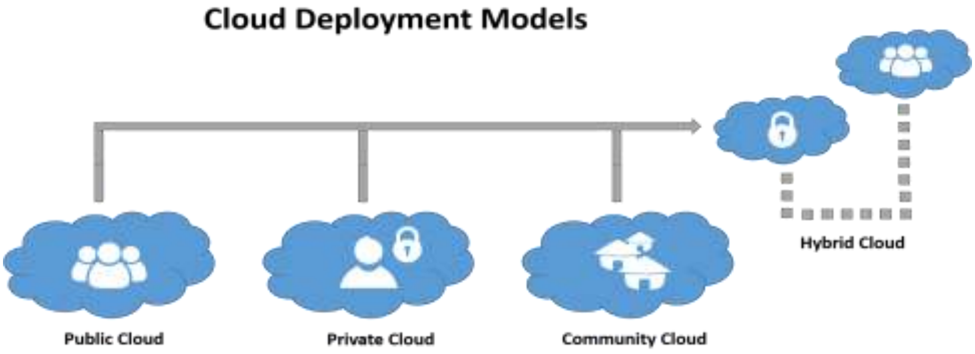

Figure 3. Deployment Types

NECESSARY CHARACTERISTICS OF CLOUD COMPUTING

Cloud technology is in the news quite often these days, but it still seems to be mysterious and confusing to the non-techie crowd [7]. Cloud options are enticing various industries across the board, which is why it's important to know its essential characteristics as a software offering. Here are the five main characteristics that cloud computing offers businesses today.

i. **On-demand self-service:-**A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

ii. **Broad network access: -** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

iii. **Resource pooling: -**The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

iv. **Rapid elasticity: -** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

v. **Measured service: -** Cloud systems automatically control and optimize resource use by leveraging a metering capability1 at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

IMPORTANCE OF SECURITY IN CLOUD COMPUTING

The power, flexibility and ease of use of CC comes with lot of security challenges. Even though CC is a new intuitive way to access applications and make work simple, there are a number of challenges/issues that can affect its adoption. A non-exhaustive search in this field reveals some issues. They are: Service Level Agreements (SLA), what to migrate, security, etc. Cloud Computing has a feature of automatic updates, which means a single change by an administrator to an application would reflect on all its users. This advertently also leads to the conclusion that any faults in the software are visible to a large number of users immediately, which is a major risk for any organization with little security.

It is also agreed up on by many researchers that security is a huge concern for adoption of cloud computing. A survey by IDC on 263 executives also shows that security is ranked first among challenges in CC. Even though a company boasts to have top class security and does not update its security policies from time to time, it will be prone to security breaches in near future.

SECURITY CONCERNS IN CLOUD COMPUTING

a.Users authentication: User authentication process must be improvised to ensure that malicious users do not get access to powerful computing systems in cloud computing.

b.Leakage of data or Data loss: Data can be at risk if an unauthorized person gains access to shared pool of resources and deletes or modifies data. This risk can increase further if there exists no backup for that data.

c.Clients trust: There must be strong authentication practices implemented to ensure that the client's data is being protected from unauthorized access.

d.Malicious users handling: Malicious users can be attackers using cloud services with a malicious intent or an insider who has gained the trust of company but works to gain access to sensitive information stored in cloud [1].

e.Hijacking of sessions: These kind of attacks happen when a legitimate user is prone to phishing or insecure application interfaces that can be exploited by attackers. Through this kind of attacks, attackers gain user credentials and hijack legitimate users sessions [3].

f.Wrong usage of CC and its services: Cloud computing service providers give access to try their cloud services for a limited period of time for free. Some users utilize this trial period to misuse the resources obtained through CC service provider [2].

RELATED WORK

Dinesh Devkota et.al (2015): In this research work, the author introduces a new security mechanism that will enforce cloud computing services against breaches and intrusions. Existing techniques for securing servers used for cloud computing and storage of data has also been surveyed. In addition to these techniques, a newly developed technique for security in cloud-based servers (MIST) has been described.

Neha Kajal et. al (2015) : This research work has analyzed the various security aspects that are vulnerable to the cloud computing and needed to be resolved. This will help to upgrade promising benefits of cloud computing so that consumers cannot have a second thought regarding its adoption.

Mehdi Ezzarii et.al (2015): The research work focuses on the performance of intrusion detection solutions (IDS) by analyzing their performance in terms of recognition, security and capacity. The main aim of this research work is to help engineers to implement adequate solution (IDS) depending on the security levels of cloud computing. The proposed method is based on two-stage.

Priyanka Ora et. al (2015) : In this research work, a solution is provided to maintain data security and data integrity. This scheme contains a combination of RSA Partial homomorphic and MD5 hashing algorithm .In this solution data is encrypted by RSA Partial before uploading it on cloud server. After uploading its hash value is calculated by MD5 hashing scheme.

Nivedita Shimbre et. al (2015) : The research work discusses the file distribution and SHA-1 technique. When file is distributed then data is also segregated into many servers. So here the need of data security arises. Every block of file contains its own hash code, using hash code which will enhance user authentication process; only authorized person can access the data. Here, the data is encrypted using advanced encryption standard, so data is successfully and securely stored on cloud. Third party auditor is used for public auditing.

Vinay Kumar et.al (2015): The author describes how to secure data and information in cloud environment in time of data sharing or storing by using cryptography and steganography technique. Cloud computing is based on network and computer applications. In cloud data sharing is an important activity. Small, medium, and big organization are use cloud to store their data in minimum rental cost. In present cloud proof their importance in term of resource and network sharing, application sharing and data storage utility.

Tejinder Sharma, et.al, [2013]: in this paper author discuss about the cloud computing. As, the computer networks are still in their infancy, but they grow up and become sophisticated. Cloud computing is emerging as a new paradigm of large scale distributed computing. It has moved computing and data away from desktop and portable PCs, into large data centers. It has the capability to harness the power of Internet and wide area network to use resources that are available remotely. There are many security issues in the cloud computing.

Sonal Guleria, Dr. Sonia Vatta, (2013): describes that the Cloud computing is emerging field because of its performance, high availability, least cost and many others. In cloud computing, the data will be stored in storage provided by service providers. Cloud computing provides a computer user access to Information Technology (IT) services which contains applications, servers, data storage, without requiring an understanding of the technology. An analogy to an electricity computing grid is to be useful for cloud computing.

Pradeep Bhosale et.al, (2012): discuss that today's world relies on cloud computing to store their public as well as some personal information which is needed by the user itself or some other persons. Cloud service is any service offered to its users by cloud. As cloud computing comes in service there are some drawbacks such as privacy of user's data, security of user data is very important aspects. In this paper author discuss about the enhancement of data security. Not only this makes researchers to make some modifications in the existing cloud structure, invent new model cloud computing and much more but also there are some extensible features of cloud computing that make him a super power.[9]

Jasmin James, et.al, (2012): discuss about the security in cloud computing. Cloud computing is fast growing area in computing research. With the advancement of the Cloud, many new possibilities are coming into picture, like how applications can be built and how different services can be offered to the end user through

Virtualization. There are the cloud services providers who provide large scaled computing infrastructure defined on usage, and provide the infrastructure services in a very flexible manner.

RESEARCH MOTIVATION

In this research work, we will try to enhance Security between the client and cloud accessing the cloud. No doubt, cloud has got multiple benefits but we should not forget that there is a high risk of data getting confidential information getting leaked. In order to avail the benefits of cloud, we must ensure the security of data being transferred between the client and user.Security is the key for the Cloud success, security in the cloud is now the main challenge of cloud computing. Until a few years ago all the business processes of organizations were on their private infrastructure and, though it was possible to outsource services, it was usually non-critical data/applications on private infrastructures. Now with cloud computing, the story has changed. The traditional network perimeter is broken, and organizations feel they have lost control over their data. New attack vectors have appeared, and the benefit of being accessible from anywhere becomes a big threat.

- No secure authentication: In the present work, there is no secure authentication procedure defined. When you log on to your machine and then try to access a resource, say a file server or database, something needs to assure that your username and password are valid. With sensitive data stored in the cloud of the different users, we need a strong authentication mechanism. Data breaches because of no/weak authentication.

- No Gateway is defined: The user should not be directly connected to the cloud provider as there is high risk of data getting stolen or hacked by the third party intruder. There is a requirement of gateway/broker that acts as an intermediate between the cloud provider and the client.

- No Read/Write policies have been defined. Different privileges should be given to the different types of users.

CONCLUSION

With the continuous growth and expansion of cloud computing, security has become one of the serious issues. Cloud computing platform need to provide some reliable security technology to prevent security attacks, as well as the destruction of infrastructure and services. There is no doubt that the cloud computing is the development trend in the future. Cloud computing brings us the approximately infinite computing capability, good scalability, service on-demand and so on, also challenges at security, privacy, legal issues and so on. But to solving the existing issues becomes utmost urgency. To protect against the compromise of the compliance integrity and security of their applications and data, firewall, Intrusion detection and prevention, integrity monitoring, log inspection, and malware protection. Proactive enterprises and service providers should apply this protection on their cloud infrastructure, to achieve security so that they could take advantage of cloud computing ahead of their competitors. These security solutions should have the intelligence to be self-defending and have the ability to provide real-time detection and prevention of known and unknown threats. To advance cloud computing, the community must take proactive measures to ensure security.

REFERENCES

[1] D. Devkota, P. Ghimire, D. J. Burris and D. I. Alkadi, "Comparison of Security Algorithms in Cloud Computing," IEEE, pp. 1-7, 2015.

[2] N. Kajal , N. Ikram and P. , "SECURITY THREATS IN CLOUD COMPUTING," IEEE, pp. 691-694, 2015.

[3] M. EZZARII, H. E. GHAZI, H. ELGHAZI and T. SADIKI, "Performance Analysis of a Two Stage Security Approach in Cloud Computing," IEEE, 2015.

[4] P. Ora and D. Pal, "Data Security and Integrity in Cloud Computing Based On RSA Partial Homomorphic and MD5 Cryptography," IEEE International Conference on Computer, Communication and Control (IC4-2015), 2015.

[5] N. Shimbre and P. P. Deshpande, "Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES algorithm," IEEE, pp. 35-39, 2015.

[6]V. k. pant, J. Prakash and A. Asthana, "Three Step Data Security Model for Cloud Computing based on RSA and Steganography Techniques," IEEE, pp. 490-494, 2015.

[7] Y. Zhu and J. Zuo, "Research on Data Security Access Model of Cloud Computing Platform," IEEE, pp. 424-428, 2015.

[8] Tejinder Sharma, Vijay Kumar Banga. Efficient and Enhanced Algorithm in Cloud Computing, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-1, March 2013

[9] Sonal Guleria1, Dr. Sonia Vatta2, to enhance multimedia security in cloud computing environment using crossbreed algorithm, Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com, Volume 2, Issue 6, June 2013

[10] M. Brantner, D. Florescu, D. A. Graf, D. Kossmann, and T. Kraska. "Building a database on s3. In J. T.-L. Wang", editor, ACM, pages 251–264, 2008.

[11] S. H. Brown. "Multiple linear regression analysis: A matrix approach with matlab". Alabama Journal of Mathematics, 2009.

[12] Alawode A. olaide, "On Modeling Confidentiality Archetype and Data Mining in Cloud Computing", IEEE, African Journal of Computing and ICT, March 2013.

[13] Himeldev, Tanmoysen, "An Approach to Protect the Privacy of Cloud Datafrom Data Mining Based Attacks", IEEE.

[14] Vishal Jain, "Information Retrieval through Multi-Agent System with Data Mining in Cloud Computing", IJCTA, January 2012.

[15] Neha Tirthani: "Hellman and elliptical curve cryptography, Proceedings of TCC", volume 3378 of LNCS, pages 325-341. Springer-Verlag (2005)

[16] Amar Gondaliya : "Security in Cloud Computing", Technical Paper Contest 2011.

[17] Anthony Bisong, "An Overview of the Security Concerns in enterprise Cloud computing", International Journal of the Security Concerns in Enterprise Cloud Computing, 2011.

[18] R. Kalaichelvi Chandrahasan, "Research Challenges and Security Issues in Cloud Computing", International Journal of Computational Intelligence and Information Security, March 2012 Vol. 3, No. 3.

[19] Vahid Ashktorab, "Security Threats and Countermeasures in Cloud Computing", International Journal of Application or Innovation in Engineering and Management, Vol 1, Issue 2, October 2012.

[20] Mandeep Kaur, "Using encryption algorithms to enhance the data security in Cloud computing", International journal of communication and computer technologies, Vol 1, No 12, 2013.

[21] Mr. Tejas P. Bhatt, "Security in Cloud Computing using File Encryption", International Journal of Engineering Research and Technology, Vol. 1 Issue 9, November 2012.

[22] Eng. Anwar J. Alzaid and Eng. Jassim M. Albazzaz, "Cloud Computing Challenges and related Security Issues", 2009 A sur vey Paperhttp://www.cse.wustl.edu/~jain/cse571- 09/ftp/cloud/index.html

[23] A. Raja Rajeswari and R.Sakkaravarthi , "Top Threats to Cloud Computing V1.0" , March 2010

[24] T.V. Mahendra, "Data Mining for High Performance Data Cloud using Association Rule Mining", International Journal of Advanced Research in Computer Science and Software Engineering, January 2012.

[25]. Bhagyashree Ambulkar, "Data Mining in Cloud Computing", MPGI National Multi Conference 2012.

[26] Eng. Anwar J. Alzaid, "Cloud Computing: An Overview", International Journal of Advanced Research in Computer and Communication Engineering, September 2013.