CLOUD COMPUTING: SECURITY FEATURES AND COMPLIANCE

SAMPATHKUMAR.D[1], SMITHA.M[2], ABDOUL ELBASTOI SAIDABDOU [2],
ASSISTANT PROFESSOR [1], STUDENT [2], DEPARTMENT OF COMPUTER TECHNOLOGY
SRI KRISHNA ARTS AND SCIENCE COLLEGE, COIMBATORE, TAMIL NADU, INDIA

ABSTRACT

Cloud computing is coming the term that describes the means of delivering any and all Information Technology components-from computing power to computing infrastructure, applications, business process and collaboration-actually offering IT as a service. Cloud computing is an emerging style of computing where data, applications, and resources are provided to users as services over the Web.There are two technologies they are Multi-tenancy, Virtualization which provides securityfeatures about cloud computing.

Keywords: Virtualization, Multi-tenancy

INTRODUCTION

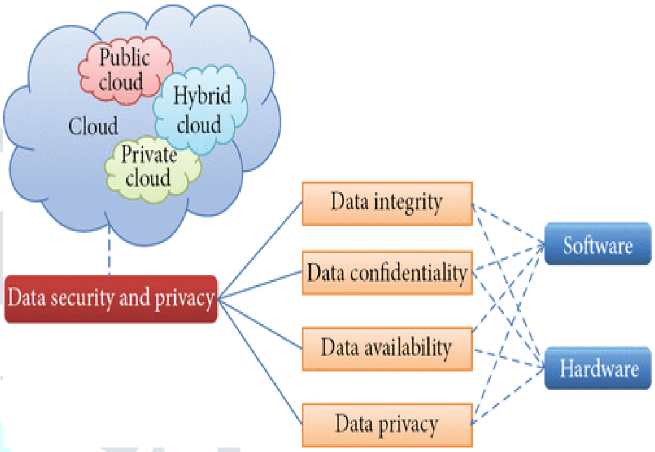
Cloud computing security denotes to the set of processes, procedures and standards designed to provide information security assurance in a cloud computing environment.Cloud computing security includes both physical and logical security issues across all the different service models of software, platform and infrastructure. It also shows how these services are delivered (private, public or hybrid delivery model). cloud security provides a wide range of security services from an end-user and cloud provider's perspective, where the end-user will primarily will be concerned with the provider's security policy, how and where data is stored and who has access to that data. For a cloud provider, on the other hand, cloud computer security problem can range from the physical security of the infrastructure and the access control mechanism of cloud assets, to the execution and maintenance of security policies.

TOP5CLOUD COMPUTING SECURITY FEATURES

When a user searches for a cloud service provider, he or she needs to make sure that it must have these five cloud computing security features:

FEATURE 1: ADVANCED PERIMETER FIREWALL

Most of the firewalls are simple because they just examine the source and destination packets only. However, there are having more advanced firewalls available that perform stable packet inspection. It will check the file packets integrity to ensure the stability before selecting or rejecting the packet.



The top-of-the-line firewalls, for example, Palo Alto Networks' perimeter firewall, which will check the data stored in the file packet in order to examine the file type including source, destination, and integrity. This quality is really necessary to prevent the most advanced persistent threats.

FEATURES 2: INTRUSION DETECTION SYSTEMS WITH EVENT LOGGING

All IT security commands standards must involve the businesses to have a means, which can track and record all type of intrusion attempts. Thus, IDS event logging solutions are important for all businesses that want to meet the commands standards like **PCI** and **HIPAA.**

There are few cloud distributors, who offer IDS monitoring service and update the security rules for their firewalls in order to counter the threat signals and malicious IP addresses, which are detected for all cloud users.

FEATURES 3: INTERNAL FIREWALLS FOR EACH APPLICATIONS& DATABASES

Using a powerful or top-in-line perimeter firewall will stop the external attacks only but internal attacks are still a major danger. However, if there are no internal firewalls in infrastructures to avoid the sensitive data access and applications is not considered secure. For example, an employee user account hacker can easily bypass the perimeter firewall completely.

FEATURE4:DATA-AT-REST ENCRYPTION

Data encryption is one of the most powerful methods to keep the most sensitive data stored in the cloud computing infrastructure safe and secure from the unauthorized person. More than that, strong type of encryption will minimize the chance of stolen data used for some purpose. In addition, a user has an ability to alert them and they can take steps to protect their individuality.

FEATURE 5: TIERIV DATA CENTERS WITH HIGH PHYSICAL SECURITY

Last possible way for the hackers and the industrial spies is the physical hardware, which is used to run a cloud environment to steal the most important data. If hackers get direct access to the hardware, which runs the cloud they have free reign to rob the data or upload the virus directly to the local machine.

Thus, a user must use tier IV data centers that will prevent the cloud environment and stop the access to the physical systems. A secure tier IV data centers utilize measures like:

- 24X7 CCTV monitoring
- Controlled access checkpoints via biometric security controls
- Armed security patrols

These security measures are efficient for keeping unauthorized parties away from directly accessing to the hardware through which cloud is running.

If a user has five cloud computing security features, then businesses can ensure that the selected cloud solution will prevent them from almost all internal and external threats. However, there are some other threats also that can badly obstacle the cybersecurity in the cloud. Thus, to defeat all type of cloud threats, a user is advised to use the solutions provided by Cloud Codes in all possible cases. It is one of the majority cloud data security solution providers among the business users.

SECURITY ADVANTAGE OF CLOUD BASED SYSTEM

DATAENCRYPTION

Robust data encryptions within cloud-based security systems have substantially reduced the possibilities of data breaches; these solutions offer a layered approach that consists of security, key management, intelligence and secure access controls. Cloud-based systems provide the required freedom to companies to choose their users who will be accessing the data that has been outsourced to the cloud. This way, any attempts to alter with personal or profession data can be accomplished.

Most companies face the threats of internal data theft by their employees, and stronger access controls can nip these threats in the bud. The multi-layered security features bring out the possibilities of a breach of data to a great extent. Data, irrespective of its type, needs to be prevent at all times. Any violations can be danger to the goodwill and the functioning of an enterprise.

AVOIDDDOSATTACKS

Distributed Denial of Service (DDoS) attacks can result in great losses for entertainment companies. Hackers target the website by directing traffic from several sources to the end website, as a result, the system gets overwhelmed. These DDoS attacks may tarnish the image of the company, as clients begin to lose trust on the company. Cloud-based security systems guard this immediate threat with real-time scanning of potential risks; this function is further used as a warning tool for the various systems which allows for the tracking of incoming threats and attacks instantly – this enables website owners to divert the traffic to several different locations.

REGULATORYCOMPLIANCE

Cloud computing security solutions usually provide reliable SOC1 and SOC2 certifications to the entertainment businesses regarding cloud computing. These certifications ensure periodic security of data and all types of possible glitches. Cloud-based solutions manage the requisite infrastructure for regulatory compliance and the protection of information. Detailed **AmazonWebServices[AWS]** reports about management of security controls ensure all organizations focus on their business operations, without worrying about compliance requirements.

SECURESTORAGE

Traditional storage solutions do not provide any protection against possible disasters that have enough capacity to erase required data from devices. Cloud computing allows the users to store their data in a secure manner, thereby negating any mishaps that may affect the equipment. Cloud storage solutions offers private, public, and hybrid solutions which the businesses may choose as per their requirements and needs. The hybrid cloud storage systems allow the users to keep their data more secure in the most effective manner.

PATCHMANAGEMENT

The vulnerabilities of a website are mostly exploited by hackers to breach the security system of a company. Cloud service providers keep their sites updated; further on, they ensure that no vulnerabilities appear. Moreover, cloud solutions offer real-time assistance to clients by providing companies with the option to scale cloud solutions during high traffic circumstances. This facility willallow companies to reduce their cost of services substantially.

These large number of security features are quite flexible, agile, and comfortable. Enhanced security features offer sufficient protection to the private and financial information of both media and entertainment companies and help to thwart data and intellectual property breaches. In this long and distinct period of digitalization, where cybercrime has emerged as a norm, cloud-based solutions seem to be the best alternative to traditional security systems.

SECURITY DISADVANTAGE OF CLOUD BASED SYSTEM

CLOUD DEPLOYMENTS MODELS

In the cloud deployment model, networking, platform, storage, and softwareinfrastructure areprovided as services that scale up or down depending on the demand as depicted in The Cloud Computing model has three main deployment models they are:

PRIVATE CLOUD

Private cloud isa new term that some marketers have recently used to describe offerings that emulate cloudcomputing on private networks. It is set up within an organization's internal enterprise information center. In the private cloud, larger resources and virtual applications are the two provided by the cloud vendor are pooled together and available for cloud users to share and use. It differs from the public cloud because all the cloud resources and applications are managed by the organization itself, similar tofunctionality of Intranet. Utilization of the private cloud can be much more secure than that of the publiccloud becauseof itsspecified internal functionality. Only the organization and designated stakeholders of authorized persons mayhave access tooperate ona specific Private cloud.

PUBLIC CLOUD

Public cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisionedon a fine-grained, self-service basis over the Internet, via web services/web applications, from an off-site unauthorized-party provider who shares resources and bills on a fine-grained utility computing basis. It is commonly based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes indemandfor cloud optimization.Public clouds have less securitythan the other cloud models because it places an additional burdenof ensuringall applications and data accessedon the public cloud are not subjected to malicious attacks.

HYBRID CLOUD

Hybrid cloud is a private cloud linked to one or many external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network.It provides virtual IT solutions through a combination of both public and private clouds. Hybrid Cloud provides more secure control of the information and applications and allows various parties toaccess data over the Internet. It also has an open architecture that allows interfaces with other management requirements. Hybrid cloud can describe configuration combining a local devicesuch as, a Plug computer with cloud services. It can also describe configurations combining virtual and physical, collocated assets -for example, a mostly virtualized environment that requires routers, physical servers, or other hardware such as a network appliance acting as a firewall or spam filter.

METHODS TO ENSURE SECURITY IN THE CLOUD

ORGANIZATIONAL SECURITY RISKS

Malicious Insiders. The risk of having malicious personnel in a Customer ServicePoint[CSP] staff can be mitigated by putting strict legal constraints in contracts when hiring personnel. A comprehensive help of the **CustomerServicePoint** by a third party as well as a robust security breach notification process will also go a long way to preventing this.

PHYSICAL SECURITY RISKS

Physical Breach, the risk of intruders gaining physical access to devices used in the provision of cloud services can be reduced by having strong physical security deterrents in place they are armed guards, key card access and biometric scans to stop access to sensitive locations in the data centre.

TECHNOLOGICAL SECURITY RISKS

Virtualized defense and reputation based trust management - CSP could use the following structure: a hierarchy of **Distributed Hash Table[DHT]**-based overlay networks with specific tasks to be performed by each layer. The lowest layer deals with widespread aggregation and probing colluders. The highest layer deals with various attacks. Reputation aggregation here is related to utilizing various sources to verify certain connections and probing colluders refers to checking if any sources are associated with known unauthorizedparties. Secure virtualization - CSP can use an Advanced Cloud Protection system (ACPS) to ensure the security of guest virtual machines and of distributed computing middleware. Behavior of cloud components can also be monitored by periodic checking loggingof executable system files. Trust model for security and interoperability - There should be separate domains for providers and users, each with a special trust agent. A trust agent is an independent party that collects security information and data used to verify an endpoint. There should also have many different trust strategies for service providers and customers.

COMPLIANCE AND AUDIT RISKS

This area primarily deals with legal issues and as such, both CSPs and Computer Science Corporation need to understand legal and regulatory obligations and ensure that any contracts made meet these obligations The CSP should also ensure that its discovery capabilities do not satisfy security and privacy of data. Having seen some methods used to protect lapses in security from the other four areas, in the next subsection we will look at some of the primary techniques used for ensuring the information and data security.

CONCLUSION

Cloud computing is a promising and emerging technology for the next generation of IT sectors. The barrier and difficultiestowardthe fastgrowthofcloudcomputingaredata security and personal issues. Decreasing data storage and processingcostisamandatoryrequirementofanyorganization, while analysis of data and information is always the very most importanttasksinalltheorganizationsfordecision making. Sonoorganizationswilltransfertheirdataorinformationto the cloud until the trust is built between the cloud service providers and consumers and they are very confidential. A vast 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 techniquesmoreeffective and productive.Moreworkisrequiredinthearea ofcloudcomputingtomakeitacceptedbythecloudservice consumers. This paper surveyed different techniques about data security and privacy, focusing on the data storage and useinthe cloud, dataprotectioninthecloudcomputing environmentstobuildtrustbetweencloudserviceproviders andconsumers.

REFERENCE

[1] N. Leavitt, “Is cloud computing really ready for prime time?” Computer, vol.42,no.1,pp.15–25,2009.

[2] P.MellandT.Grance,“Thenistdefinitionofcloudcomputing,” National Institute of Standards and Technology, vol. 53, no. 6, article50,2009.

[3]F.Berman,G.Fox,andA.J.G.Hey,GridComputing:Makingt heGlobalInfrastructureaReality,Volume2,JohnWileyandsons , 2003.

[4] M. A. Shah, R. Swaminathan, and M. Baker, “Privacy-preservingauditandextractionofdigitalcontents,”IACRCryptologyEPrintArchive,vol.186,2008.

[5] Z.XiaoandY.Xiao,“Securityandprivacyincloudcomputing,” IEEE Communications Surveys & Tutorials, vol. 15, no. 2, pp. 843–859,2013.

[6]N.Kshetri,“Privacyandsecurityissuesincloudcomputing:theroleofinstitutionsandinstitutionalevolution,”TelecommunicationsPolicy,vol.37,no.4-5,pp.372–386,2013.

[7] R.Latif,H.Abbas,S.Assar,andQ.Ali,“Cloudcomputingrisk assessment: a systematic literature review,” in Future InformationTechnology,pp.285–295,Springer,Berlin,Germany,2014.

[8] A. Aviˇzienis, J. Laprie, B. Randell, and C. Landwehr, “Basic conceptsandtaxonomyofdependableandsecurecomputing,”IEEETransactionsonDependableandSecureComputing,vol.1, no.1,pp.11–33,2004. [9] Z. Mahmood, “Data location and security issues in cloudcomputing,”inProceedingsofthe2ndInternationalConference onEmergingIntelligentDataandWebTechnologies(EIDWT’11), pp.49–54,IEEE,September2011.

computing,”inProceedingsofthe2ndInternationalConference onEmergingIntelligentDataandWebTechnologies(EIDWT’11), pp.49–54,IEEE,September2011.

[10] D. Sun, G. Chang, L. Sun, and X. Wang, “Surveying and analyzing security, privacy and trust issues in cloud computingenvironments,”inProceedingsoftheInternationalConferenceon AdvancedinControlEngineeringandInformationScience(CEIS ’11),pp.2852–2856,chn,August2011.

[11] Pandey, R. M. Tugnayat, and A. K. Tiwari, “Data Security Framework for Cloud Computing Networks,” International JournalofComputerEngineering&Technology,vol.4,no.1,pp. 178–181,2013.

.