IJRESM
International Journal of Research in Engineering, Science and Management
Volume-1, Issue-12, December-2018
www.ijresm.com | ISSN (Online): 2581-5792

Security in Cloud Computing

S. Prashanth[1], Rakshith Gowda[2], Chanchal Antony[3]
[1,2]Student, Department of Computer Science Engineering, Alva's Institute of Engg. and Tech., Moodbidri, India
[3]Sr. Assistant Professor, Dept. of Computer Science Engg., Alva's Inst. of Engg. and Tech., Moodbidri, India

***Abstract*: Cloud computing has changed the world around us. Now people are moving there data to cloud since data is getting bigger needs to be accessible from many devices. "How much secure is cloud computing?" .Noting that security is one of the main barrier for continuing growth of cloud computing. In this paper, we discusses the security of data in cloud computing. It is a study of data in the cloud and aspects related to its security. The main objective is to identify major security risks and issues which are needed to think about during implementation and development of services in cloud and the way how to reduce those security risks and issues. However, it is important to know that, cloud computing is not insecure, it just needs to be managed and accessed securely.**

***Keywords*: Cloud Computing**

1. Introduction

Cloud Computing is the name given to the recent trend in computing service provision. Of the several definitions which are available, one of the simplest is, "a network solution for providing inexpensive, reliable, easy and simple access to IT resources" Cloud Computing is considered as service oriented. This service oriented nature of Cloud Computing is cost effective and also provides flexibility and improved performance to the end user.

In 1950's it was a gradual evolution started with mainframe computing. After sometime, around 1970, the concept of virtual machine was created. The VM operating system took the 1950's shared access mainframe to the next level, permitting multiple distinct computing environments to reside on one physical environment.in 1990's telecommunication companies started offering virtualized private network connections.in late 90's the term "cloud computing "is coined by professor Ramanath Chellappa in a talk on a "new computing paradigm", in 2002 Amazon created Amazon Web Services(AWS), providing an advanced system of cloud services from storage to computation. In 2009 Google apps also started to provide cloud computing enterprise applications. Now Soft Layer is one of the largest global providers of cloud computing infrastructure.

A major concern in adaptation of cloud for data is security and privacy. It is very important for the cloud service to ensure the data integrity, privacy and protection. For this purpose, several service providers are using different policies and mechanism that depend upon the nature, type and size of data.

One of the advantages of Cloud Computing is that data can be shared among various organizations. However, this advantage itself poses a risk to data. In order to avoid possible risk to the data, it is necessary to protect data warehouse.

One of the key problems while using cloud for storing data is whether to use a third party cloud service or create an internal organizational cloud. Sometimes, the data is too sensitive to be stored on a public cloud, for example, national security data or highly confidential future product details etc.

This type of data can be extremely sensitive and the consequences of exposing this data on a public cloud can be serious. In such cases, it is highly recommended to store data using internal organizational cloud. This approach can help in securing data by enforcing on-premises data usage policy. However, it still does not ensure full data security and privacy, since many organizations are not qualified enough to add all layers of protection to the sensitive data.

2. Background of cloud computing

A. *Cloud computing*

Cloud computing refers to promising model of computing technology where machines with large data centers can be dynamically provisioned, arranged, controlled and reconfigured to deliver the benefits in adaptable way. Most `cloud computing services are provided self service and on demand, so even vast amounts of computing resources can be provisioned in minutes, typically with just a few mouse clicks giving a lot of flexibility.

B. *Characteristics of cloud computing*

1) *On-demand self- services*

A consumer can singularly provision computing capabilities, for example server time and network storage, when needed automatically without requiring human interaction with each service provider.

2) *Broad network access*

Cloud services are available over the network, therefore a standard mechanisms are used to provide services on heterogeneous platforms.

3) *Resource pooling*

It is an IT term used in cloud computing environments to describe a situation in which providers serve multiple clients, customers or "tenants" with provisional and scalable services. The idea behind resource pooling is that through modern scalable systems involved in cloud computing and software as a service (SaaS), providers can create a sense of infinite or immediately available resources by controlling resource adjustments at a meta level. This allows customers to change their levels of service at will without being subject to any of the limitations of physical or virtual resources.

4) Rapid elasticity

Companies sometimes require additional resources in a little timeframe and this is where cloud computing comes in to play. For instance, in case a firm gets a fresh client and needs three extra servers to meet up the customer's business requirements, the service provider could allow the firm to maintain three unique servers at a time.

5) Measure usage

The measure usage characteristic represents the ability of a cloud platform to keep track of the usage of its IT resources, primarily by cloud consumers. Based on what is measured, the cloud provider can charge a cloud consumer only for the IT resources actually used and/or for the timeframe during which access to the IT resources was granted. Measured usage is not limited to tracking statistics for billing purposes.

C. Service delivery models

1) Software as a Service (SaaS)

Sometimes said as 'on-demand software', SaaS is a software licensing and delivery model wherever a complete functional and complete software product is delivered to users over the net. SaaS offerings are typically accessed by end users through an internet browser making the user's operating system mostly irrelevant and can be billed based on consumption, with a flat monthly charge. SaaS offerings are the most widely visible of all the cloud computing service models. In fact, many users might be using SaaS products without even realizing it. Cloud providers install and operate application software within the cloud and cloud users access the software from cloud clients. Cloud users do not manage the cloud infrastructure and platform where the application runs. This eliminates the need to install and run the appliance on the cloud user's own computer that simplifies maintenance and support.

2) Platform as a Service (PaaS)

Platform as a Service is a category of cloud computing that provides a platform and environment to allow developers to create applications and services over the net. PaaS services are hosted in the cloud and accessed by users simply via their internet browser. What developers gain with PaaS may be a framework they can build upon to develop or customize application. PaaS makes the development, testing, and preparation of applications fast, simple, and cost-effective. With this technology, enterprise operations, or a third-party provider, can manage operating system, virtualization, servers, storage, networking, and therefore the PaaS software itself. PaaS is sometimes called 'middleware', referring to how it conceptually sits somewhere between SaaS and IaaS.

3) Infrastructure as a Service (IaaS)

IaaS is the lowest-level cloud service paradigm IaaS model is an instant computing infrastructure, provisioned and managed over the Internet. Rapid scale all over with demand and pay just for what you utilize. IaaS helps you to avoid the expense and complexity of buying and managing your own physical servers and other datacenter framework. Each resource is offered as a separate service segment and you only need to rent a particular one that you require it. The cloud computing service provider deals with the framework, while you purchase, install, manage your own software—operating systems, middleware and applications.

Table 1
Layer and examples

Layer	Examples
Client	Computers, phones, other electronic devices, operating systems and browsers.
Application (SaaS) .	Computers, phones, other electronic devices, operating systems and browsers.
Platform (PaaS)	Google App Engine, Force.com, Windows Azure, WOLF.
Infrastructure (IaaS)	Virtual servers leased by Amazon, Rackspace, Go Grid.
Server	Multi-core processors, cloud-specific operating systems and combined offerings.

D. Cloud computing deployment models

There are three fundamental deployment models for cloud computing environment but NIST (National Institute of Standards and Technology) proposed four set of deployment models.

1) Public clouds

In this model of cloud infrastructure represents a cloud environment which is publicly accessible and manageable by an organization or a third party cloud service providers. The public cloud deployment model have the unique advantage of being significantly more secure than accessing information via the Internet and tend to cost less then private clouds because services era more commoditized.

2) Private clouds

This model of infrastructure is managed and operated only by private organization. The primary goal of this type of cloud model is to sustain consistent level of security and privacy. The private cloud allows for increased security, reliability, performance, and service.

3) Community Cloud

This type of model shares infrastructure between organizations or communities have common mission and vision such as: security, jurisdiction. Services are managed by organizations or third parties. The community members generally share similar privacy, performance and security concerns. The main intention of these community's is to achieve their business-related objectives.

4) Hybrid Cloud

This type of deployment model is composition of two or more cloud models, they are bound together but each of them remains unique entities. NASA is one example of a federal agency who is utilizing the Hybrid cloud computing deployment model.

3. Threats in cloud services

There are numerous security issues for cloud computing as it surrounds many technologies including networks, databases, operating systems, virtualization, resource programming, dealing management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing.

The security issues found within the cloud are

1. Abuse and Criminal use of Cloud Computing
2. Insecure Application Programming Interfaces
3. Malicious Insiders
4. Shared Technology Vulnerabilities
5. Data Loss/Leakage

1) Abuse and criminal use of cloud computing

The issue arises due to relatively weak registration systems present in cloud computing environment the Permitted CSPs may be abused for wicked purposes, supporting criminal or other unwanted activities towards consumers. As an example, services may be used to host malicious code or used to facilitate communication between remote entities i.e. botnets. The stress is that authorized services are used with malicious intent in mind. Other issues seen includes supplying of purposefully insecure services used for data capture.

Service providers could provoke potential users with offers too sensible to be true. For example the promise of unlimited resources. During the registration process the consumer will be asked to provide more data than what would usually be needed under the aspiration of providing service personalization.
E.g. location or age based advertisement.

Commonly asked data includes the consumers name, email/postal address, D.O.B or even credit card details. Users are essentially being provoked to give up more information than required as a necessity for service use. Malicious entities will then use this data for criminal purposes. Even though the entities don't seem to be malicious the declaration of data to the CSP can also be said to be an abuse of service by the CSP themselves. CSPs could collect this data, or the other data provided at later stages, and market this data to third parties for data processing purposes.

2) Insecure application programming interfaces

Cloud computing providers expose a set of software interfaces or API's that customers use to manage and interact with cloud services .Data placed within the Cloud will be accessed through Application Programming Interfaces (APIs) and other interfaces. Malfunctions and errors within the interface software system, and conjointly the software system used to run the Cloud, can lead to the unwanted exposure of user's data. Data exposure may also occur once a software system malfunction affects the access policies governing user's data. This has been seen in several Cloud based services in which a software malfunction resulted in which a user's privacy settings were overwritten and therefore the user data exposed to non-authorized entities. Threats may also exist as a results of poorly designed or implemented security measures. If these measures are non-existent, the software system may be simply abused by malicious entities. APIs and other interfaces need to be made secure against accidental and malicious attempts to avoid the APIs and their security measures. Few examples are unknown access or reusable tokens or passwords, clear-text authentication or transmission of content, inflexible access controls, limiting monitoring and logging capabilities. Remediation: analyze the security model of the cloud provider interfaces, understand the dependency chain associated with the API.

3) Malicious insiders

The threat of malicious insiders is well-known to most organizations. The threat is boost for consumers of the cloud services by the convergence of IT services.

Although a CSP may be seen as being honest their staff may not be honest. A malicious insider is an employee of the CSP who abuses their position for information gain or for other criminal purposes. e.g. dissatisfied employee. Regardless, of the employee's motivation the worrying side is that a secretive employee will have access to consumer's information for authorized purposes but will abuse this power for their own methods. Another more noticeable form of the malicious insider problem is through PaaS based services.

If the service provider offers a platform that permits developers the power to interact with user's data i.e. Facebook Applications, users may unknowingly allow these developers to access all their data. Use of this platform could also be unchecked. For example, it is well known on the Facebook platform that once a user adds an application the application will have the power to access all the users information, if allowed to try so, no matter the applications operate. Remedies are Enforce strict supply chain management and conduct a comprehensive supplier assessment, specify human resource requirements as a part of legal contracts, determine security break notification process.

4) Shared technology vulnerabilities

A more interesting form of confidentiality issue relates to the development of a cloud and services themselves.

- *Virtualization Issues:*

The underlying virtualization design allows IaaS service providers the ability to host many machine pictures on one server. First, the authors showed that they could map the internal structure of the cloud, allowing them to determine if two virtual machines were co-resident with each other i.e. we're running on the same physical machine. Secondly, they demonstrated that they were able to, purposefully, add a virtual machine to the cloud so that it was co-resident with another machine. Finally, the authors were ready to show that once a machine was co-resident, they might be ready to launch several attacks that may permit them to learn information regarding CPU cache use, network traffic rates and keystroke timings.

- *Service Aggregation*

Aggregated services offer services based upon the functionality offered by existing services. Often Aggregated services offer the combined functionality of existing services providing rapid service construction. However, service aggregation presents consumers with several interesting problems. Data is now being shared across multiple service providers whose privacy policies will also subject to alter. Under whose privacy policy is the data governed by, how to combine the two policies? moreover, service aggregation can occur in an emergency and rapid manner implicit that less demanding controls could have been applied to the protection of data, increasing the probability of a problem. Remedies are Implement security best practices for installation/configuration. Monitor environment for unauthorized changes/activity, Promote strong authentication and access control for administrative access and operations. Enforce service level agreements for patching and vulnerability remediation, Conduct vulnerability scanning and configuration audits.

5) Data loss or leakage

There are many ways to compromise data. Deletion or alteration of records without a backup of the original content is an obvious example. Unlinking a record from a larger context may render it unrecoverable, as can storage on unreliable media. Loss of an encoding key may result in effective destruction. Finally, unauthorized parties must be prevented from gaining access to sensitive data. The threat of data compromise increases in the cloud, due to the number of and interactions between risks and challenges which are either unique to cloud, or more dangerous because of the architectural or operational characteristics of the cloud environment. Few examples are insufficient authentication, authorization, inconsistent use of encryption and software keys, rational failures, persistence and remenance challenges: disposal challenges, risk of association; jurisdiction and political issues, data center reliability. Remedies are Implement strong API access control, Encrypt and protect integrity of data in transit, Analyzes data protection at both design and run time, Implement strong key generation, storage and management, and destruction practices, Contractually demand providers wipe persistent media before it is released into the pool, Contractually specify provider backup and retention strategies.

4. Cloud security risks

The security risks associated with each cloud delivery model vary and are dependent on a wide range of factors including the sensitivity of information assets, cloud architectures and security control involved in a particular cloud environment.

Security risks in cloud computing are

A. Privileged user access

Cloud providers generally have unlimited access to user data, controls are needed to address the risk of privileged user access leading to compromised customer data.

B. Data location and segregation

Customers may not know where there data is being stored and there may be a risk of data being stored alongside other consumer’s information.

C. Data disposal

Cloud data deletion and disposal is a risk, particularly where hardware is dynamically issued to customers based on their needs. The risk of data not being deleted from data stores, backups and physical media during de-commissioning is enhanced within the cloud.

D. Assuring cloud security

Customers cannot easily assure the security of systems that they do not directly control without using SLAs and having the right to audit security controls within their agreements.

E-investigations and protective monitoring the ability for cloud customers to invoke their own electronic investigations procedures within the cloud can be limited by delivery model in use, and the access and complexity of cloud architecture .Customers cannot effectively deploy monitoring systems on infrastructure they do not own, they must rely on the systems in use by the cloud service provider to support investigations.

5. Solution to data security

Encryption is suggested as a better solution to secure information. Before storing data in cloud server it is better to encrypt data. Data Owner can give permission to particular group member such that data can be easily accessed by them. Heterogeneous data centric security is to be used to provide data access control. A data security model contains of authentication, data encryption and data integrity, data recovery, user protection has to be designed to improve the data security over cloud. To ensure privacy and data security data protection can be used as a service.

To avoid access of data from other users, applying encryption on data that makes data totally unusable and normal encryption can complicate accessibility. Before uploading data into the cloud the users are suggested to verify whether the data is stored on backup drives and the keywords in files remain unchanged. Calculate the hash of the file before uploading to cloud servers will ensure that the data is not altered. This hash calculation can be used for data integrity but it is very difficult to maintain it. RSA based data integrity check can be provided by combining identity based cryptography and RSA Signature.

SaaS ensures that there must be clear boundaries both at the physical level and application level to segregate data from different users. Distributed access control architecture can be used for access management in cloud computing. To identify unauthorized users, using of credential or attributed based policies are better. Permission as a service can be used to tell the user that which part of data can be accessed. Fine grained access control mechanism enables the owner to delegate most of computation intensive tasks to cloud servers without disclosing the data contents. A data driven framework can be designed for secure data processing and sharing between cloud users. Network based intrusion prevention system is used to detect threats in real-time. To compute large files with different sizes and to address remote data security RSA based storage security method can be used.

6. Conclusion

Increased use of cloud computing for storing data is certainly increasing the trend of improving the ways of storing data within the cloud. Data available in the cloud will be in danger if not protected in a rightful manner. This paper discussed the risks and security threats to data in the cloud and given an overview of cloud computing. Virtualization is examined to find out the threats caused by the hypervisor. Similarly, threats caused by criminal use and insecure use of application and also about the data loss in cloud have been discussed. One of the major concerns of this paper was data security and its threats and solutions in cloud computing. A brief overview is also given for solution of security in cloud which includes the encryption of data, hash key and suggestion before uploading data into cloud.

References

[1] Mastering in cloud computing by Rajkumar Buyya, The University of Melbourne and Manjra soft Pvt. Ltd, Australia.
[2] Security and Privacy Issues in Cloud Computing by Jaydip Sen Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA
[3] Data Security in Cloud Computing Ahmed Albugmi Madini O. Alassafi Robert Walters, Gary Wills University of Southampton University of Southampton University of Southampton, United Kingdom Southampton
[4] Security threats on cloud computing vulnerabilities Te-Shun Chou Department of Technology Systems, East Carolina University, Greenville, NC, U.S.A.
[5] Cloud Computing Security Issues, Challenges and Solution Pradeep Kumar Tiwari1, Dr. Bharat Mishra2 M.phil (CSE)student, 2Reader in department of physical Science, at Mahatma Gandhi Chitrakoot Gramodaya Vishwavidyalaya Chitrakoot - Satna (M.P.)
[6] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham. “Security Issues for Cloud Computing.”
[7] C. S. Alliance. (2011). Security Guidance for Critical Areas of Focus in Cloud Computing V3.0.