Assessment on Security Issues and Classification in Cloud Computing

B.Mahalakshmi
Research Scholar
Department of Computing Science
Vels University
Chennai.
maha.karthik921@gmail.com

ABSTRACT:

In the cloud environment, security and privacy becomes a major concern to be addressed and it should be reliable and truthful. Likewise cloud computing is one among them where the data is outsourced to some third party cloud providers for providing service to the user in the way the resources are utilized. Even though there are lot of advantages while transiting the data through internet there are some security issues are to be considered in account. Once the problem of security and privacy occurred the user's data are lost and the resources are under the control of the malicious attacker. The cloud server and the provider need to take necessary action to avoid the threats. In this paper the detailed study about the security threats and key security issues are discussed. Different key issues are also explained such as network security issues, virtualization, security, access control, confidentially, authentication, authorization all these are discussed. The various classification and key challenges are shown in the paper.

1. INTRODUCTION:

In the current years distributed computing is a developing idea with loads of new proposed structure utilizing the mix of disseminated computing, grid computing and parallel computing. It is widely used by individuals and organization because of the flexibility and easy to access provisions available in cloud. People can use the cloud on the on-demand basis that is whatever their needs they can adopt it from the cloud and can pay only for the service which is provided by the cloud providers. The cloud is kept up by a cloud specialist co-op in which every one of the administrations are given and kept up by them.

Consumers are more flexible platform to use the cloud storage and resources with a minimal cost. Rather than owing its large number of expensive resources the consumer can buy the cloud as on-demand basic, where the cloud cost is only for the amount of user's need. The organization and the industries are very beneficiary. Different from traditional system the cloud provides some control to the user of having the control of the cloud storage where the data are stored. The virtual machines are also a major part of the cloud where the sever are virtualized to the user and provides service.

Security and privacy are the most vital critical issues that is to be mentioned in

the cloud environment which should be reliable and trustable. The data storage in cloud are outsourced to some third party providers and the user lost their control over their data and fully depends on the cloud providers for managing the data .In this paper the author explained various types of security threats and key security issues over the cloud environment[1].

The treacherous 120 cloud computing top threats is a survey done by the CSA- Cloud Security Alliance. In this they done a research work on the cloud threats which are nightmare to the customer. They conducted a survey on some top organization and some industries to know about the greatest security issues which they are facing currently. To find out the top threats they conducted survey on top industrial experts and based on the survey opinion the treacherous 12-2016 is reported. They finalized a list of 12 threats and among those the survey based threats which is giving lot of issues is considered to the first. They ranked the threats on the basis of the survey[2].

Several key terms are discussed such as vulnerability, threats, proposing taxonomy, attacks etc. and their classifications. The main content reviews are all discussed. The author tells about the several open research on the above[3].

In order to get a clear computing the author proposed the characteristics and distinguish the research area where the cloud environment has its own technical, conception, and user experience. The main characteristics of cloud are service oriented, strong fault tolerant, loose coupling, ease use and business modeling. Hence the clear insight on cloud will move on to further discussion[4].

In this paper, the creator proposed about the duping demoralization and computational convention security, or SecCloud is a convention which goes about as a scaffold for secure stockpiling and the computational reviewing in the cloud and protection swindling is finished by planned verifier signature group check and probabilistic examining procedure. The nitty gritty investigation is to limit the cost by acquiring testing size. They fabricate a handy secure mindful distributed computing natural and further the viability and productivity are to be in the proposed module[5].

1.1. OVERVIEW OF CLOUD COMPUTING

1.1.1. Characteristics

1. **On-Demand Self-Service**-Without any need of human interaction a user can have the capability to have some of the provisions such as user access, network storage and server time with a particular service provider.

2. **Broad Network Access**- Using some standard interface services over the network can be accessed from a heterogeneous platform eg. Laptops, Desktops, Mobile Phones and PDAs.

3. **Resource Pooling**- the service providers dynamically allocating and de-allocating the physical and virtual resources for the needs of the clients. These are done by the location independency and in some cases the

user can able to find the location of the resource by the abstraction provided.

4. **Rapid Elasticity**- The ability of figuring can be immediately provisioned to quick scale out and discharged to quick scale in.

5. **Measured Service**- Asset utilization can be accounted for, controlled and observed, so the client can pay the supplier for what he utilized as a part of the cloud.

1.1.2 DELIVERY MODELS

The following are the 3 service models available in cloud. The Fig 1 below represents the cloud deployment and service model along with the characteristics.

1. **Software as a Service(SaaS)**- software in the cloud are offered by on demand basis. The applications which are accessible by a web browser are available in this service model are intended to end users.

2. **Platform as a Service(PaaS)**- gives end client instruments and administration to make another application and for sending them brisk and successfully. The software's which are used to build a platform are available in this service model.

3. **Infrastructure as a Service(IaaS)**- It combined hardware and software for supporting process, Storage, networking and other computing resources to form a infrastructure.

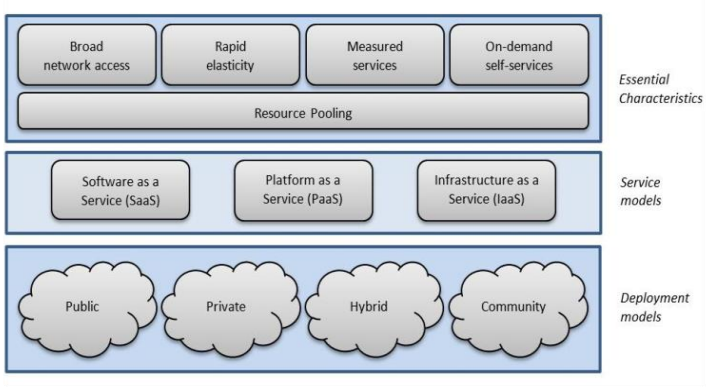


Fig 1 Characteristics of Cloud, Deployment and Service model

1.1.3 DEPLOYMENT MODELS

Public cloud- The cloud service which are available in the network is in a public mode. So that everyone can able to access the resources. Because of this the cost also controlled as all of the users are sharing the resources. E.g. Google.

Private Cloud- It is a platform for cloud resources which act as a internal cloud environment. It is protected by the particular organization by firewalls. Private cloud is only for the authorized user who can have the permission to access the data all these are controlled by the organization and have a control over the data available.

Hybrid cloud- Here the sensitive data are stored and accessed by the authorized users which are under the private cloud the remaining ordinary data are managed by the public cloud.

Community Cloud- It is working under mutual sharing among organizations which belong to some particular community. It is internally managed or externally by some third party provider. It is perfect for the business and organization which works on a

centralized cloud that can able to manage build and work with same projects.

2. SECURITY ISSUES – THE TREACHEROUS 12

The CSA provides a research report called "The Treacherous 12 - Cloud Computing Top Threats" in recent years for the organization and other experts to understand about the risk management of security issues which is currently available. The CSA carry out a survey with the industrial experts to know about the security issues which are currently facing among the organization and found top threats which are currently threatening the environment. And following the survey they ranked the threats based on the severity[6][7][8].

In the first level the research is on collecting the list of security threats by surveying with experts in organization and people who are all using cloud. Then from the list they ranked the threats based on the STRIDE and Risk management. The STRIDE research work is developed by Microsoft for evaluation of security threats which is explained below

Spoofing Identity(S): The unauthorized or unprivileged user are allowed to access someone's identity illegally such as user name and password.

Tampering with Data(T): The malevolent alteration of data are involved in data tampering. The attacker can change the data in the database without having any access rights over the internet.

Repudiation(R): The user might do a particular function, and then later deny having executed it. For example, an illegal action is performed by a user in which it lacks the ability to trace the illegal operations in a system.

Information Disclosure (I): exposing the data to an individual who are not having the access rights to do the operations such as reading a file which the user is not having the access rights to do it.

Denial of Service(D): A denial-of-service is denying access rights to the user having authorization. For eg temporarily blocking the web server so that the valid user also cant able to use the web site.

Elevation of Privilege(E): Getting access permission which is not really owned to the user is elevation of privilege. Most of them are developed to create a new threat.

2.1. SECURITY THREATS

1.Data Breaches:

It is an event where the data is sensitive, protected or secret data is accessed or viewed by unauthorized users. The sensitive data's in the organization is viewed by counterpart on attacks through the virtual machines.

2.Weak Identity, Credential and Access Management:

Due to scalability in identifying the access management system the data breach and other attacks are enabled. Because of this the failure of authentication is occurred such as week passwords lack of cryptographic keys etc.

3. Insecure APIs:

For providing different service offers to customer the cloud service providers and third parties are using the APIs. Lacking of Robust identity and access management

policy may increase the risk level and also the complexity.

4. System and Application Vulnerabilities:

For stealing the data in the system some attackers infiltrate a system by taking the control or disturbing the operations system vulnerability is awakened.

5. Account Hijacking

Exploitation, phishing and fraud vulnerabilities are used for the attackers to gain the access of the customer credentials and to launch subsequent attacks.

6. Malicious Insiders

Thrid party providers , system administrators, current or former employees, contractors who are having the access rights will misuse and will cause damage to the sensitive datas in the organization which is having the confidentiality , availability and integrity.

7. Advanced Persistent Threats (APTs)

This is a bloodsucking type of digital assaults that penetrates framework to start a grasp in target organizations accessible in the cloud foundation for carrying the information and licensed innovation.

8. Data Loss

Information which are put away in the cloud can be lost because of a portion of the coincidental ways such as loss of encryption key, deletion, or some of the physical catastrophe such as fire, flood, earthquake etc.

9. Insufficient Due Diligence

While adapting to new technology without understanding the work of service provider and not having proper assessment of the operations in and out which may leads a critical situation to the organization.

10. Abuse and Nefarious Use of Cloud Services

Poor cloud service security, free trials to the cloud service and some fraud account signing through payments can expose the cloud computing models SaaS, PaaS, IaaS to malicious attack.

11. Denial of Service

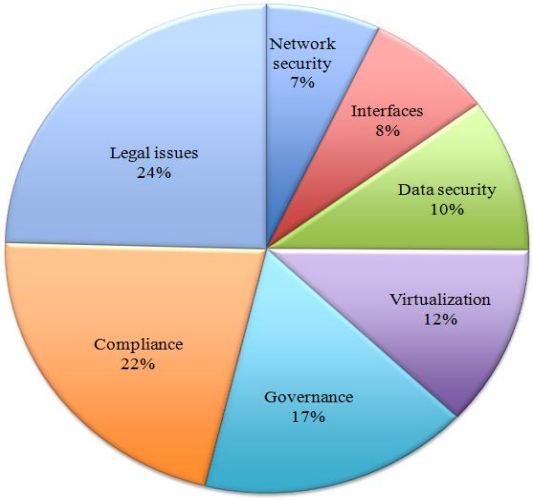
The attackers create a huge amount of false request to a particular cloud server , because of this the server needs to consume more power for processor, disk space, memory, network bandwidth. So the system gets slower and keeps the service shut for other users.

12. Shared Technology Issues

The shared technologies attacks such as hypervisor vulnerability, VM sprawl, VM cross channel attack and many are the possible threats available in the cloud. Because of this the shared multitenant architecture can expose a potential compromise to the entire environment.

3. SECURITY THREATS AND VULNERABILITIES:

In this section some of the major key security issues are discussed and grouping them into six categories such as Network Security, Virtualization and Hypervisor Security, Identity and Access Management, Data and Storage Security, Governance, and Legal and Compliance issues. The graph 1 represent the overall analysis of key security threats.



Graph 1. Overall Graphical representation of Key Security issues.

3.1 Network security

Many organization and companies are facing the network issues while using the resources thorough network. So here some of the key issues which are associated with network communication and configurations of the cloud computing resources are discussed [9][10].

3.1.1. XML Signature (Wrapping Attack)

The protocol Simple Object Access Protocol- SOAP is accessed by having the authentication purpose and integrity through the XML signstures. The protocol which it uses the XML signature endure from an known attack is XML signature wrapping or simply wrapping attack. For web services a predefined part of protocol is signed using the XML signature for ensuring the communication integrity. The information is having a security header along with an element which shows one or more parts of the signed message. The Wrapping attack in essence uses the signature element which does not pass on any message about the mentioned part of the message. Hence the attacker can able to modify the message structure and infuse malicious code without quashing the signature. The attacker nearly wraps the XML signature around the malicious code and passes it on as if it were an authentic message.

3.1.2 Flooding Attacks

Whenever the company's computational demand rose the virtual machines are allotted instantaneously by the cloud to manage the demand[10]. This would leads the malicious attacker to get in to use the feature. By creating a huge number of virtual achiness lead to create a fake quest and send to the client server. But it is the server to validate the request carefully. Because of this the entire network flooded with request and waiting for the server to response, so that it leads to DDoS attack.

3.1.3. Malware Injection Attack

Implementing a malicious server or installing virtual machines are thinks getting injected in the cloud server. The attacker's aim to create a service of his own by implementing the malicious script or code for deploying the services in the cloud so that it looks like a legal service. If this gets successful then the operations are done in the server which they intend to perform. Hence when a request is send to the cloud server it redirects to the malware server so that the attackers implement their service[11]. The impact of the attack such as unauthorized access resources of cloud, eavesdropping, subtle modification of data, functionality changes, user credential leakage and service blocking. The challenge is to detect the malicious server and keep the virtual machine safe from the malware injection attack.

3.1.4.Metadata Spoofing Attack

At the time of communication with some other web services a client need to gather all the information necessary for

invoking a web service. This includes the details such as address of the web service, message format, location of the network, security needs etc which are available in the metadata provided by the web server. The most common metadata credentials are WSDL- Web Service Definition Language and WSSecurity-Policy. Using the communication protocols such as HTTP or E-Mail are used for metadata documents and some possibility of spoofing attacks are opened. The attacker can maliciously in WSDL, spread across all clients. The attacker modify the file of WSDL the endpoints of network and the security policies. In cloud environment the metadata spoofing is very dangerous where the cloud system itself having some WSDL functionality. New user can get some WSDL file and spread the malicious WSDL file throughout the network.

3.1.5 Insecure APIs

The cloud customers are using a APIs Application Programming Interfaces for managing and make interaction with the cloud service. Application management, enabling security functions, service provisioning etc are all done with these interfaces. It is easily targeted by the malicious attacker if the identity and access management are not properly designed. The attacker is trying to enter the security system and create the vulnerability in these APIs using some insecure policies. It becomes more complicated because the organization needs to share their credentials for the user to enable the services. Organization provides an unsecured APIs that can expose to variety of threats such as integrity, accountability, confidentiality and availability.

3.1.6 Cross Site Scripting (XSS) Attack

The Cross Site Scripting (XSS) which affect the malicious script to the web content of someone else so that they can force the website to execute the codes of the attackers. The attackers target the end user of the website and he is the victim to get the vulnerable acts. The root cause of XSS attack is that not validating the user input properly. Because of this the neutralization of website and incorrect validation is occurred in the website. This is the key for the attackers to steal the cookies, obtaining the online user credentials, extracting the sensitive data and also many malicious activities. The XSS can retain the full control in the web browser as like Trojan-horse programs. The two ways of getting affected is that opening the pop-up screen or link which is created by the malicious attacker or just visiting a web page which is created by the malicious attacker in the web page. So that the attacker can gets the control over the sensitive data.

3.1.7 SQL injection Attack

Hence the attacker can able to have the unauthorized access to databases. The attacker can able to modify the data deleting, updating without the knowledge of the cloud server as it pretending like a authorized person. The attacker can also change the access rights to someone for modifying the data which results in complete destruction. The key reasons for the attacks are SQL is generated dynamically and inadequate handling of user input. These are all the reasons behind the attack.

3.2 Virtualization and Hypervisor Security

In cloud computing virtualization is one of the core component where the organization use their application in a cost effective way. The security component is also to give the services such as monitoring virtual machines performance management,

capacity management and cloud infrastructure management. Hypervisor performs the abstraction layer by giving essential resource management functions between the virtual machines for sharing resource of the hardware. Here some of the virtualization threats are explained[12][13][14].

3.2.1 Hypervisor Vulnerabilities

VMs and application simultaneously on a single machine and to segregate the VMs. Sometimes hypervisor are vulnerable to some attacks. If the attacker can able to control the hypervisor then all the data under VMs are under the control of attacker. Hypervisor is a potential target for the hackers so that it is easy for them to get the control of lower layers of virtualized environment. Since hypervisor having the control of host OS the difficulty is to detect the attacks using normal security measures are not possible.

3.2.2 VM Escape

The VM are designed to sustain strong segregation between the VMs and host. But damage to the system makes the attackers to insert some malicious program. When it runs the attacker breaks the segregated boundaries and started the operating system directly by the VMM Virtual Machine Monitor. Hence the attacker gain the host machine and do some attacks.

3.2.3 VM Sprawl

Without having control and doesn't have proper management the VM sprawling occurs in the VM. Even the system retains some resources during the time they cannot be assigned to someone and lost. VM is usually allotted by the user and the acknowledgement has to be created by the system in response. The problem is after the completion of VM the data are lost while transit. The user creates some new request and it will cause to grow number of VMs so the entire system gets collapsed. Moving the orphan VMs to some other server also cause some problem in the security level, QoS and privacy challenges.

3.2.4 Cross VM Side Channel Attack

For the maximum resource utilization the physical server contains multiple VMs in the cloud environment and this leads to VM side channel attack. The malicious gertr into virtual and collapse the data between the VMs, access to the hardware and cache locations are getting damaged. While the malicious attacker enters into the virtual machine they create many problems such as Cross VM side attack, DoS, remote monitoring etc. through tiing interference. It is possible for the attacker to retain some fine grained data also result in cross VM side attack.

3.2.5 Single Point of Failure

The VM environment is based on the hypervisor method so that the control over the VMs physical and the overall functions are controlled by it. So the over usage of hypervisor will leads to collapse the overall system which is done by software faults and overuse of infrastructure. Because of this the arbitrary state corruptions are occurred and all the data in the VMs are lost. Virtualized server are having lots of access point so that the attacker can easily enter into the virtual cloud to exploit the system that is VMs, host machine and hypervisor.

3.2.6 VM Image Sprawl

In cloud computing VM images if secure management is a most required thing.

It is having software containing all applications that are installed and configured then it is used for booting the VM into an initial stage that is some check point. These are considered as data and easy to clone. Hence the increasing number of VM cause VM sprawl. Many of the VM images frequently. There some problem occurs if the VM images warehouse is not properly maintained in that place security and privacy issues are occurred. While the data owner released some images of the VM by accidentally, the attackers will find the loopholes of the security and also can inject some malicious code to damage the VM.

3.3 Identity and Access Management (IAM)

One of the important cloud computing elements is managing the identities and keeping a secured a large scale is a greatest challenge in IT industry. For many organizations the data security as well as the privacy issues is most important. So a best identity and way in to management is a best approach for an on demand cloud computing services. The evidence of user identity and authentication feature of identity management includes the maintenance, personally identifiable information (PII) protection which is collected from the cloud clients. Therefore the discomfort unauthorized access to data resources in considered being a major concern. The following are the major IAM concerns are to be addressed for successful and effective identity management in the cloud.

3.3.1 Identity management:

The continuous change in user's role and tasks inside the organization, change in business, turnover of users are the factors which are affecting the prolong IAM process.

3.3.2 Authentication:

Another key issue is authentication of user identity and securing the system in a dependable way. Other challenges are credential management in a proper way, ensuring strong authentication, password standard compliance, encryption management and all types of cloud services.

3.3.3 Authorization and Access Control:

Another vital requirement is creating a smooth authorization and access control terms and polices for the user to access the resources. In addition to this some of the challenges are access management, cloud based identity, privileges and control over the access to resource maintaining and adapting to changes in the user role are some of them.

3.3.4 Federation Management:

By providing significant privacy and security challenges the identity information are distributed dynamically among the security domains. The week and insecure communication network leads to session hijacking, replay attacks, phishing attacks etc. Moreover trust identity management in IDP cause data breaches and theft if it behaves cruelly.

3.4 Data and Storage Security:

The third party data maintain that is data warehousing, data outsourcing has become a trend , therefore the user solely depends on the cloud service provider for the data availability, integrity and confidentiality of their data. A cloud service provider who is having the user's data are need not to be trusted hence the cloud

service provider have to be noted carefully while ensuring the data integrity with lot of attention. There are some possibilities that service provider can hide some of the lost data from the user to for maintaining their reputation that could not be damaged[15[16[17].

To exacerbate the situation the providers sometime forgot the importance of sensitive data and intentionally deleting the files which are rarely used one by the normal clients. Even though the cloud having very useful platform for the modern cloud environment it shows about the cloud storage security and performance of the entire system. That is even we are using third party outsourcing of data is very beneficiary in cloud environment there is some drawbacks such as lack of confidentiality, availability, integrity are delayed by the end user. Here some of the data and storage issues are discussed.

3.4.1 Data Confidentiality

The basic principle of confidentiality is “need to know” or “least privilege”. The important and sensitive data should be restricted for those individuals or systems that who are having precise need to access it. The quantity of access point is increased as the cloud environment is having large amount of parties, applications and devices etc. because of this the data breaches risk is increased. The possible concerns that affect the confidentiality in public Authentication and authorization that is access control method, protection of data, used encryption algorithm and last encryption key management.

3.4.2 Data Integrity:

This means the data should be reliable accurate and could not be altered delicately or modified by an unauthorized party. Integrity means the data associated with the cloud is accessed only by the authorized person and it should not be modified illegally, non repudiation and accountability. Hence the actions within the system are performed with a user. The cloud consumer should worry about the integrity of the data along with the confidentiality. A strong encryption method is used for confidentiality and for integrity the message authentication codes are used.

3.4.3 Data Availability

It is that the data should be accessible when the customer is in need of the data and its architecture. Even though the architecture is highly reliable and available the computing services can experience and slowdown. Data loss can be complete or partial so that the availability of data can be affected. While the threats quantity is increased while the availability exist. The DOS is a network based attack and the cloud service provider own availability could be another concern. More than this there are some concerns such as disk/sector failures results in permanent data loss.

3.4.4 Data Isolation

The usage of shared infrastructure could a vital concern. While concentrating on data it shows various risk associated with data and includes sharing the infrastructure with tenants who are untrusted and relying on security and availability of the infrastructure. These vulnerabilities show a significant obstacles of the cloud based services. Before transferring data to cloud the administrator have to ensure that the data in the cloud are secured and can able to access only by the authorized users. In cloud environment generally the customer request is being processed by an application with adequate rights to access. Application level is the only way to protect the data of all the

tenants which could leads to cross tenant leakage of data making the cloud less secure than the physical resources.

3.4.5 Data Sharing

The intrinsic nature of data and resource sharing shows the attractive model of cloud service for user applications such as calendaring, word processing, social networking and blogging etc. it allows multiple user to use the shared resource by editing concurrently, being scalable available and accessible. These benefits on different can affect privacy because of the server side data leakage and significant risk about the confidential of the shared resources. In cloud storing data is not adequate it should have a guarantee of secrecy. But sometimes the unrestricted secrecy can also cause a serious problem. In an organization a challenging employee can be mislead by others by sharing fake files and without being traceable. The frequent change of members in a group makes difficult while sharing the data in a multiple owner while saving..

3.4.6 Data Backup & Redundancy

In the cloud storage while outsourcing data does not mean that data is backed up actually. If the data is lost accidentally or modified by some opponent and the encryption key also lost. Recovery is possible if only the original data is backed up properly. To avoid the loss of data and also to maintain the business consumer must make sure the data is maintained by the backup polices. Because of the simple operation service providers prefer seamless backups without having consent of the client. This method is due to some internal or external. So controlling data and maintain the backup is another challenging issue and replication should be maintained.

3.4.7 Data Sanitization

The fundamental obligation of public cloud environment is about recovery of after the complete deletion of data inclusive of all log files and made the backup recovery. The timely demolition of data is very challenging since the replicated data are dispatched all over the geographical since it is difficult for the service provider to remove all the backup copies of the data. Additionally the disk which is to destroyed is shared by the clients. Sometimes it is necessary to delete the storage media ti=o ensure its work. Is it is not removed properly it can be reused by some discarded media.

3.4.8 Data Provenance

It needs to deserve some vigilant attention that data origin in cloud is one of the securities to be maintained. Provenance is nothing but the data that is who is generated, accessed and modified and the action of sequence about the data. The provenance of sensitive data is to give up the critical information and the opposition looks for the loopholes to utilize it. Data provenance is valuable where information trace-back, forensic analysis, auditing andit needs history-based access

3.4.9 Dynamic Data Updates

In cloud computing environment it is difficult to ensure about remote data integrity when the updating of data is frequently done by modification, deletion and insertion. On remote integrity the existing work checks for static data and accessible to dynamic data are more common. Some security loopholes includes direct extension of PDP that is provable data possession.

3.4. Governance

In a cloud background the consumer give up the control to the service provider for some of the critical issues which is having security implications. Here are some of the issues developed from the governance issues[18].

3.4.1 Improper Data Sanitization:

While erasing the data it should be completely erased by the service provider or else the data could be reconstructed as it consider the client is not encrypted the disk.

3.4.2 Data and Information leakage:

While transferring the data to the cloud the control over it can be backing up the data, redundancy, security policies, file system, and some other important configurations are coees under the consumers point of view.

3.4.3 Vendor Lock-in:

A consumer depends on a particular service provider means then it would be difficult to move for another service provider hence no establishment in standardized data and portability among the data and servie provider in cloud computing.

3.5 Legal and Compliance Issues

It is the responsibility of the organization to operate according to the rules and regulation of the government by following the laws, standards, regulations and specification. The following are some of the issues considered to be a concern in some place[19][20[21].

3.5.1 Data Location:

Here the data redundancy is used for storing the data in multiple ways in different geographical location and the client doesn't knowing the detailed information of the data. while the data transfers the border the administration is having variety of other security concerns.

3.5.2 Contracts and Electronic Discovery:

While dealing with electronic mode the common issues such as identification, compilation and analysis of data that is stored in the discovery phase of a lawsuit.

3.5.3 Laws and Regulations:

Laws and regulation are differing from country to country as they are having their own security and privacy laws and regulations which is complicated to handle.

4. Conclusion

This paper discusses the popular cloud frameworks ENISA, CSA, NIST have surveyed various vulnerabilities and the ranking order of the threats is surveyed. Apart from these the security issues and its classification such as network security, virtualization, APIs and some legal issues are explained. Here the key security issues and the problem faced by the customer organization are well explained. Depends upon the vulnerability the attacks are classified and the data should be confidentially maintained by the server. While doing this the issues such as authentication, authorization, integrity and confidentiality.

References

1. Islam, Tariqul, D. Manivannan, and Sherali Zeadally. "A classification and characterization of security threats in cloud computing." Int. J. Next-Gener. Comput 7.1 (2016).
2. https://cloudsecurityalliance.org/download/the-treacherous-twelvecloud-computing-top-threats-in-2016
3. Fernandes, Diogo AB, et al. "Security issues in cloud environments: a survey." International Journal of Information Security 13.2 (2014): 113-170.
4. Gong, Chunye, et al. "The characteristics of cloud computing." Parallel Processing Workshops (ICPPW), 2010 39th International Conference on. IEEE, 2010.
5. Wei, Lifei, et al. "Security and privacy for storage and computation in cloud computing." Information Sciences 258 (2014): 371-386.
6. ENISA, Cloud Computing: Benefits, Risks and Recommendations for Information Security.https://www.enisa.europa.eu/activities/risk management/files/deliverables/cloud-computing-risk-assessment.
7. Security Guidance for Critical Areas of Focus in Cloud Security Computing V3.0. http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf.
8. N. Gonzalez, C. Miers, F. RedALıgolo, T. Carvalho, M. SimplALıcio, M. Naslund, and M. Pourzandi. A Quantitative Analysis of Current Security Concerns and Solutions for Cloud Computing. In Proc. of 3rd IEEE CloudCom, 2011
9. W. Jansen and T. Grance. Guidelines on Security and Privacy in Public Cloud Computing Special Publication.http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.
10. C. Jayalath, J. Stephen, and P. Eugster. Universal Cross-Cloud Communication. IEEE Transactions on Cloud Computing, 2(2):103–116, April-June 2014.
11. I. M. Khalil, A. Khreishah, and M. Azeem. Cloud Computing Security: A Survey. Computers, 3(1):1–35,Mar. 2014.
12. P. Mell and T. Grance. The NIST Definition of Cloud Computing - Special Publication 800-145. National Institute of Standards and Technology, August 2011.
13. R. Schwarzkopf, M. Schmidt, N. Fallenbeck, and B. Freisleben. Multi-layered Virtual Machines for Security Updates in Grid Environments. In Proc. EUROMICRO-SEAA, pages 563–570, 2009.
14. R. Schwarzkopf, M. Schmidt, N. Fallenbeck, and B. Freisleben. Checking Running and Dormant Virtual Machines for the Necessity of Security Updates in Cloud Environments. In Proc. CloudCom, pages 239–246,2011.
15. R. Schwarzkopf, M. Schmidt, C. Strack, S. Martin, and B. Freisleben. Increasing Virtual Machine Security in Cloud Environments. Journal of Cloud Computing, July 2012.
16. C.Wang, Q.Wang, K. Ren, and W. Lou. Ensuring Data Storage Security in Cloud Computing. In Proceedings of the 17th International Workshop on Quality of Service, pages 1–9, 2009.
17. Cong Wang, S.S.M. Chow, Qian Wang, Kui Ren, and Wenjing Lou. Privacy-Preserving Public Auditing for Secure Cloud Storage. IEEE Transactions on Computers, 62(2):362–375, Feb. 2011.
18. Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li. Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing. IEEE Transactions on Parallel and Distributed Systems, 22(5), May 2011.
19. W. Wang, Z. Li, R. Owens, and B. Bhargava. Secure and Efficient Access to Outsourced Data. In Proc. ACM Workshop Cloud Computing Security (CCSW), Nov. 2009.

20. S. Yu, C. Wang, K. Ren, and W. Lou. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. In Proceedings of IEEE INFOCOM, 2010.
21. K. Zunnurhain and S. Vrbsky. Security Attacks and Solutions in Clouds. In Proc. 1st International Conference on Cloud Computing, page 145–156, 2010.