Security Risks: Encryption and authentication challenges in cloud data

V. Sree Rekha[1]

[1]Lecturer in Computer Science,

Sri Durga Malleswara Siddhartha Mahila Kalasala
[1]vemurisrekha@gmail.com

Abstract

As IT services has given rise to a lot of recent innovations, cloud computing is treated as maturing technology. It is internally connected with other computing technologies such as Grid Computing, Distributed Computing and Utility Computing etc. The remote server is a location where the data is stored with the help of services provided by service providers namely Amazon IBM, Google's Application provide users to access developing applications from anywhere in cloud environment. As the data is transmitted to the remote server through a channel like internet there is a need to provide security. The asset of any organisation is data itself so before implementing cloud computing in an organisation, security challenges need to addressed. Otherwise security issues may affect both the providers and consumers of the cloud services. The issues are related to the safety of the data flowing through the cloud and being stored in the cloud including data access, data availability and data privacy. To provide security for the data organisation developed certain procedures such as data encryption and service authentication schemes to deal with data in cloud computing. In order to know the problems in cloud computing technology we need to first understand the concepts behind it. This paper summarises the technological concepts and security issues related to cloud computing. It also explore challenges and facilities of infrastructure faced in cloud computing.

Keywords: Innovations, Computing Technologies, Grid Computing, Distributed Computing, Utility Computing, Remote Server, Channel, Service Provider, Infrastructure.

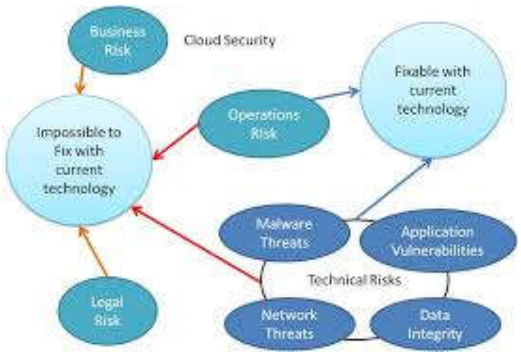

Figure1. Problems with risks in cloud data

Cloud Computing : Infrastructure, Services and Models

The computing which is based on internet that allows end users to share information and resources like networks, servers, storage, applications and services. The infrastructure is in such a way that it grasps security problems occurred during data processing in cloud computing. The cloud service includes the amount of resources exposed over a network which depend on the type of service that a vendor provide to their customers. The security services differ and to handle them with responsibility is the major task.

Services

The services are majorly classified into IaaS, PaaS and SaaS. The models are namely public cloud, private cloud, community cloud and hybrid cloud.

IaaS- Infrastructure as a Service

The infrastructure provided by vendors is computer physical hardware which includes central processing unit, network connectivity and data storage. The vendor can share their hardware between multiple customers as a part of cloud service by using virtualization software. It allows customers to run desired software applications and also make customers run, control and maintain the operating system along with the physical computer hardware. Here customer and vendor both are responsible for handling own data security and also for physical security using physical devices being used as infrastructure.

PaaS- Platform as a Service (PaaS)

The vendor provides service for the customers to use operating system and server applications along with infrastructure. It also makes vendors to use web applications or software so that the vendor controls and maintains the physical computer hardware, server applications and operating system whereas customer only controls and model, the vendor provides not only infrastructure as a Service, but also the operating systems and server applications that their customers use. Nowadays customers are more worried about security and hence the vendor responsibility is to maintain and develop the data access, data storage and network connections. The vendors include Microsoft Windows, Amazon Web Services and Google App Engine.

SaaS- Software as a Service (SaaS)

The vendors provide customers with software applications using their cloud platforms and cloud infrastructure. Users access the end user applications through web browser without any need to maintain or install additional software. The customers control and maintain specific application configuration settings whereas vendors control and maintain the physical computer hardware, software applications and operating system. Here vendor is mainly responsible for all forms of security in this service such as Google Gmail, Google Docs and Microsoft Office.

Security principles	Risks	Cloud service models (SaaS, PaaS and IaaS)		
Confidentiality	Insider user	SaaS	PaaS	IaaS
	External attacker	SaaS	PaaS	
	Data Leakage	SaaS	PaaS	
Integrity	Data segregation	SaaS	PaaS	
	User access	SaaS	PaaS	IaaS
	Data quality	SaaS	PaaS	
Availability	Change management	SaaS	PaaS	IaaS
	Denial of Service	SaaS	PaaS	IaaS
	Physical disruption			IaaS
	Exploiting weak recovery procedures	SaaS	PaaS	IaaS

Table1 : Security Principles and risks in cloud service models

Security Risks

Cloud computing gives users the ability to store data Technology keeps on advancing, providing new utilities but also grow number of potential threats. There is a need to update the data and solve solutions for certain problems that occur in computing process. Security is a major consideration for the stored data to access in cloud. Due to storage of large amounts of data using cloud computing, there is a need to secure the stored data. So certain security risks are identified commonly in cloud computing technology to reduce the insecurity towards the stored data in real time applications.

Insufficient identity, credential, and access management

Few bad actors such as operators or developers can read, modify and delete data, issue related to management functions may arise and there may be a chance of reduction of identity through unauthorized access to data and potentially damage data of end users.

Insecure Application Programming Interfaces (APIs)

APIs are used by customers use to manage and interact with cloud services. The interfaces are designed to protect data against accidental and malicious attacks to the given policy. Attacks may occur due to the storage of data without any security which leads to the damage of data resided in cloud data. These act as the major insecurity due to usage of the API on cloud data in large amounts.

Data breaches

A data breach involve some kind of information that was not intended for public release, including personal health information, trade secrets, intellectual property and simply the result of human error and poor security practices. The risk of data breach varies in cloud computing depending upon different parties for different reasons but it consistently ranks as a top for cloud customers.

System vulnerabilities

The interruption among service operations may lead to generate bugs in the program where attackers can use to control the system. These programs can effect the components of the operating system with all the services and risk of securing the stored data. In the cloud if multi-tenancy is introduced then systems from different locations can be given access to the memory and shared resources.

Account hijacking

The attackers can know the user credentials and may try to gain access the data that is stored in cloud. Though the cloud data is secure if the user enters the authorized data into the system to access stored data then cloud service provides the information as the credentials are matched with the given data checked from their database. If the attackers gain access then they can manipulate data transactions and manipulate data as per their needs and enter falsified information. The service instances may become a new base for attackers. With the knowledge of credentials attackers can often access crucial areas of computation in cloud service. instances might become a new base for attackers. With stolen credentials, attackers can often access allowing them to compromise integrity and availability of those services.

Malicious insiders

The malicious insider may be a system administrator who can access sensitive information and can have the higher level of access to the critical system and also access data present in the system. The systems that only depend on cloud service providers for security are at greater risk.

Advanced Persistent Threats (APTs)

APTs are a form of cyber attack that infiltrates systems of target companies to establish a foothold from which they steal data in the IT infrastructure. They adapt security measures to defend over extended period of time against their goals. The cyber security is a major advancement to restrict unauthorised access of data from the system which in turn depends on data security mechanism which help in data protection in the current technology.

Data loss

The stored data can be lost for several reasons other than malicious attacks in the cloud. There is a need to take measures for the accidental or deletion of data by the service provider for the sudden interruption leads to permanent loss of date due to fire or earthquake. Hence there is a need to back up data that is stored in cloud for further recovery of data which is most important in cloud.

Insufficient due diligence

In order to create business strategies, service providers and cloud technologies must be considered. Developing a checklist for due diligence while evaluating technologies and providers is essential for attaining success. To adapt cloud technologies and choose providers without performing due diligence leads to number of risks.

Abuse and nefarious use of cloud services

Few resources include email spam, phishing campaigns and distributed denail-of-services are misused. Cloud services available at free of cost through, secured cloud service deployments and fraudulent account sign-ups through payment instrument fraud lead cloud computing models to malicious attacks. There is a need to access the cloud services in a proper manner so that no one can misuse them in cloud deployment mechanism.

Denial of service (DoS)

Some of the attacks are designed to prevent users of a service DoS attacks are designed to prevent users of a service from being able to access their data or applications. By forcing the targeted cloud service to consume inordinate amounts of finite system resources such as processor power, memory, disk space, or network bandwidth, attackers can cause a system slowdown and leave all legitimate service users without access to services.

Shared technology vulnerabilities

Cloud technology divides the "as-a-service" which offers without changing the off -the-shelf software or hardware due to the expense of security. In multi-customer applications, the underlying components of cloud services may not design to offer the strong isolate properties for multi-tenant architecture. can lead to shared technology vulnerabilities that can potentially be exploited in all delivery models.

Conclusion

The understanding of cloud technology in storing large amounts of data and it's access as per the needs where security plays a vital role. The cloud infrastructural model represents various needs of the people surrounding the cloud. There are several services implemented in the current technology. The security risks are measured in various ways to protect data from unauthorized data in the cloud data. Building on that understanding we proceeded to outline and examine the various security issues that emerge as a result of the structures used in the development of various cloud computing solutions. We have realized that the bulk of issues occur in public clouds and relate to the security of the data that CSCs transmit to CSPs and vice versa. We then undertook a brief examination of some methods utilized by industry to combat the various security issues faced.

References

- Latif, R., Abbas, H., Assar, S., Ali, Q., "Cloud computing risk assessment: a systematic literature review", Future Information Technology, pp. 285-295, Springer, Berlin, Germany, 2014., URL: http://www.researchgate.net/profile/Haider_Abbas8/publication/259221049_Cloud_Computing_Risk_Assessment_A_Systematic_Literature_Review/links/0a85e53328b478e2cb000000.pdf
- Australian Government Cyber Security Operations Center, "Cloud Computing Security Considerations", September 2012, URL: http://www.asd.gov.au/publications/protect/Cloud_Computing_Security_Considerations.pdf
- Xiao, Z., Xiao, Y., "Security and privacy in cloud computing," IEEE Communications Surveys & Tutorials, vol. 15, no. 2, pp. 843-859, 2013, URL: http://mbanat.net/Security%20and%20Privacy%20in%20Cloud%20Computing.pdf
- Bhadauria, Rohit, Sanyal, Sugata, "Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques", Intl. Journal of Computer

Applications, Vol. 47, No. 18, pp. 47-66., Foundation of Computer Science, New York, USA, URL: http://arxiv.org/pdf/1204.0764.pdf

- Dahbur, K., Mohammad, B., "A Survey of Risks, Threats and Vulnerabilities in Cloud Computing.", Int Conference on Intelligent Semantic Web-Services and Applications, 2011, URL: http://www.jisajournal.com/content/4/1/5
- Ahmed, M., Hossain, A., "Cloud computing and security issues in the cloud", IJNSA, Vol.6, No.1, January 2014., URL: http://airccse.org/journal/nsa/6114nsa03.pdf
- Spoorthy, V., Mamatha, M., Kumar, S., "A Survey on Data Storage and Security in Cloud Computing", IJCSMC, Vol. 3, Issue. 6, June 2014, pp.306 - 313., URL: http://www.ijcsmc.com/docs/papers/June2014/V3I6201444.pdf
- Sen, Jaydip - "Security and Privacy Issues in Cloud Computing", Innovation Labs, Tata Consultancy Services Ltd., Kolkata, India. 2013, URL: http://arxiv.org/pdf/1303.4814.pdf
- Ukil, A., Jana, D., Sarkar A., "A security framework in cloud computing infrastructure", IJNSA, Vol.5, No.5, September 2013,pp 11-24., URL: http://airccse.org/journal/nsa/5513nsa02.pdf
- Agudo, Isaac, Nunez, David, Giammatteo, Gabriele, Rizomiliotis, P., Lambrinoudakis, Costas, "Cryptography Goes to the Cloud", Secure and Trust Computing, Data Management, and Applications, pp. 190-197. Springer Berlin Heidelberg, 2011., URL: http://www.eng.it/ricerca/file/2011%20Crypto_STAVE.pdf
- Krishna, Vamsee, Yarlagadda, Ramanujam, Sriram, "Data Security in Cloud Computing", Journal of Computer and Mathematical Sciences, Vol.2 (1), pp 15-23, 2011., URL: http://compmath-journal.org/dnload/VAMSEE-KRISHNA-YARLAGADDA-and-SRIRAM-RAMANUJAM/CMJV02I01P0015.pdf
- Cloud Security Alliance, "Security Guidance for Critical areas focus in Cloud Computing v3.0", 2011, URL: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
- Jain, Raj, "Network Access Control and Cloud Security", CSE 571s, Washington University in Saint Louis, URL: http://www.cse.wustl.edu/~jain/cse571-14/ftp/l_16nac.pdf
- Soofi, Amin, Khan, M., Fazal-e-Amin, "Encryption Techniques for Cloud Data Confidentiality", International Journal of Grid Distribution Computing, Vol.7, No.4, pp.11-20 2014. URL: http://www.sersc.org/journals/IJGDC/vol7_no4/2.pdf