Security Issues in Public Clouds

A V S ADITYAVARDHAN
Indian Institute of Information Technology Kottayam
Email: avsadityavardhan18bcs@iiitkottayam.ac.in

Yashwanth Deshaboina
Indian Institute of Information Technology Kottayam
Email: yashwanth2019@iiitkottayam.ac.in

***Abstract*—Cloud Computing delivers hosted cloud services over the internet. Computational services are usually limited but can be extended by purchasing, maintaining and updating the provided equipment. These services are accessed via HTTP(S) protocols. They can be established within a shorter time with high throughput. Costs depend on service providers. Technology advancements over the past few years have increased the security of users in the public cloud. Still, the public clouds are not 100 percent secured. More robust challenges are still underlying these public cloud accounts. This paper focuses on providing a review of different public cloud security issues and immediate remedies to date.**

I. Introduction

Majority of the Information Technology Industries directly or indirectly uses cloud services. In day-to-day life, an employee uses Gmail / Microsoft Outlook to send emails to other people in their organisation. Gmail and Microsoft Outlook are Software as a Service (SaaS) applications. Such SaaS application provides services to the end-users over the internet with some handling fee based on the account type. These SaaS applications are deployed in the cloud and use Simple Mail Transfer Protocol (SMTP) to deliver emails.

Constructing and maintaining computational resources in an IT Industry is a costly effort. It requires a lot of human effort, capital and space. IT Industry outsources its needs to public cloud computing services.[1] These are relatively cheaper and effective compared to the traditional services. Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) are three commonly categorized cloud delivery services in the market.

A. Infrastructure as a Service

Infrastructure as a Service is an instant computing infrastructure, provided and managed over the internet. In IaaS, the service provider provides support to users to manage their Operating System, Middleware applications, Runtime and Application Data. Virtualization, Servers, storage and networking will be controlled by the service provider. Amazon Web Services (AWS) offer IaaS solutions to the users. These resources are monitored for billing purposes.

B. Platform as a Service

Platform as a service provides the platform to users. Users develop, run, and manage their applications without maintaining the infrastructure. The service provider provides the Runtime, Middleware software, Operating System, Virtualization, Servers, Storage and Networking to the users. Users can control their applications and maintain them on the platform. Google Cloud Platform (GCP) offer PaaS solutions to the users.

C. Software as a Service

Software as a Service provides software to the end-users. Users don't need to run, maintain the application. Users can use software for their activities. Application, Data, Runtime, Middleware software, Operating System, Virtualization, Servers, Storage and Networking control will be in the hands of the service provider. All Cloud hosted application software comes under this delivery model. Gmail / Microsoft Outlook comes under SaaS delivery.

Users are free to adopt any delivery model to outsource their work. Each delivery model has its pros and cons but our scope is limited to cons here under security. Data / Program we insert in the cloud service providers are encrypted. Data Encryption doesn't mean that our data is completely safe. It is just a lock to make original data invisible. Once the lock is opened with a valid key, the data is visible to everyone.

As long as data is made publicly available on the internet relevant measures have to be taken care of before permitting users to see the data. Data Access Control Strategies are increasing day-by-day starting from a secured authentication systems to IP address-based authentication systems. These systems are very complex and hard to construct but are being improved to a greater extent because of the increase in number of attacks. The further sections in the paper are categorized as follows.

II. Data Security in Public Cloud

Cloud computing uses multiple technologies including but not limited to networking, databases, resource scheduling, virtualization, transaction management, load balancing, concurrency control, operating systems and memory management

In a high level there are 6 major areas where we encounter security issues in public cloud [2]

Cryptographic Encryptions can secure the data at rest as well as data in transit. But the data encryption time becomes overhead. User Authentication and Integrity protection mechanisms ensure data availability to the customer requested. These are equally important as the data is handled over the internet.

Cloud providers prefer Virtual Machines and Hypervisor to separate the cloud users. Each cloud user must have their legal and regulatory experts to inspect cloud provider's policies and practices for ensuring their adequacy. Automated notifications

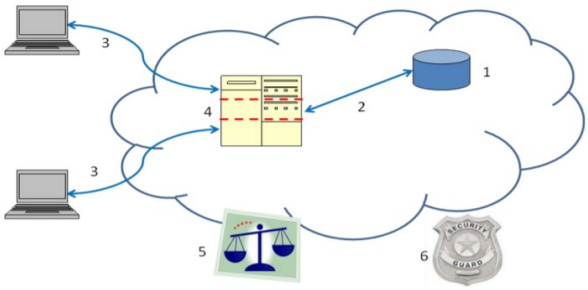

Fig. 1. 1. Data at rest, 2. Data in transit, 3. Authentication, 4. Separation between customers, 5. Cloud legal and regulatory issues and 6. Incident response.

help to inform the cloud users regarding the incident to handle the security breach.[3]

Security issues in cloud computing are dynamic. Some of the security issues are addressed below.

A. Privileged User Data Access

The customer data present in the cloud can be accessed by other cloud users in unauthorized ways. It is similar to hacking a OTP from a bank account to perform a transaction by a bank employee. These Privileged users can present inside or outside of your cloud environment but they have access to the data to manipulate.

It is one of the major issues in any database implementation. This problem was faced earlier by Apple and Google. They have mitigated this issue by the separation of duties. They have ensured that the activities of privileged third parties are monitored by your staff and fraudulent activity will make a notification to the higher authorities.[4]

B. Data Location and Segregation

Public Cloud Service providers offer multiple locations to the customer to store data. Amazon Web Services has around 100 data centers spread across 15 cities in 9 countries. Without knowing the presence of the data location, the provision of the data protection act for some region might be severely affected and violated. This also possess a risk of data along with other customers' information[5]. Segregation methods like Encryption and Digital Signatures might help to save the data.

C. Data Loss

Data in the cloud is distributed. If one data center failed to retrieve your data, another data center can access and get your data. Data loss is referred to when valuable or sensitive information on a computer is compromised due to theft, human error, viruses, malware, or power failure. User authorization and time-to-time resource monitoring can help to mitigate data loss. Swim-lane isolation is a popularly known technique that can help to avoid data loss in public clouds.[6]

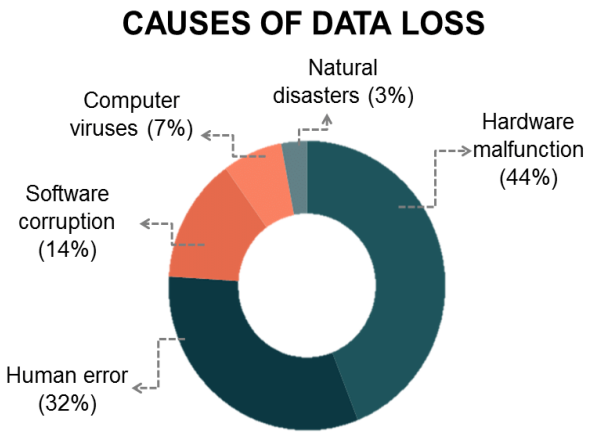

Fig. 2. Causes of Data Loss[6]

D. Data Disposal

Data Disposal refers to the deletion of user data in the cloud environment. This issue arises due to the dynamic allocation of hardware resources to cloud users. The cloud providers need to ensure that all backup, logs data must be removed alongside the user data in the cloud. Formatting the data disk drives would be an ideal option but necessary care has to be taken to make sure that other customers' data won't be affected. Improper disposal leads to side-channel attacks.

E. Protective Monitoring

Cloud users have to be monitored to protect other users data. Many privacy issues will arise but it is as important as protecting security to other users. Customers may not invoke their protective mechanisms as they are a bit costly to handle and some cloud providers don't provide service to the customer level.

III. Network Security in Public Clouds

Cloud services are offered using Networking Protocols. Cloud Service providers need to ensure a low data loss during the data transfer from local machines to the cloud environment.[7] To ensure data loss, we can use strong encryption techniques such as Secure Socket Layer (SSL) and Transport Layer Security(TSL). AWS protects users from several network attacks like Man-In-The-Middle (MITM) attack, port scanning, IP spoofing..,

A. Virtual Private Networks

A single vendor organisation can experience lower data transfer rates. Virtual Security Gateways and multiple vendors can be incorporated for high data transfer rates. This provides customer-controlled security. A private infrastructure can be established where the cloud control lies within the organization.[8]

B. Network Accessibility

Data in the public cloud can be accessed by most of the users. Eg: A public AWS EC2 server can be called in a web browser with the IPv4 address provided. A server administrator can use his security key and instance key (.pem file) to login into the server from Command Line Interface(CLI). Complex and secured User Authentication systems can help cloud users to protect the data leak. System administrators must limit the instance login access from the IP address as well. This can be performed under the security groups of AWS EC2.

C. Data Latency

Low data latency should be maintained to avoid attacks during the data transfer. Data transfer won't be continuous and consistent in the case of Metropolitan Area Networks(MAN) and Wide Area Networks(WAN) compared to LAN(Local Area Network). More number of intermediate network components affect the data latency.[9] This issue can be mitigated by invoking optimized routes to route the data from the local machine to the data center.

IV. Recent Threats in Public Clouds

Majority of the security threats arises due to the vulnerable design of cloud architecture. Poor architecture causes data loss to cloud customers. Four major security threats identified in recent times are discussed below

A. Compromised Credentials

User Credentials in public clouds compromises. It happens involuntarily a lot. For Eg: In Amazon Web Services, an email notification will be sent to the root account if a Identity and Access Management (IAM) access and secret keys are exposed publicly in the internet. It happens when we push the code into public repositories like Github, BitBucket..., Majority of the attackers get access to credentials here. A good practice is to make these credentials invalidate if the accounts are not being used. One more practice is that to provide limited access and restricted scope to these credentials.[10]

B. Data Breach

Data Breach is referred to when confidential information is stolen/used by unauthorized personnel. Data Breach can be avoided by restricting access to the information as soon as possible before the confidential information is out. It is always advised to maintain confidential data restricted to a specific set of users in the organisation. Known and trusted parties should have access to the information in the cloud. Alert systems should trigger in time of data breach.

C. Hacked Application Protocol Interfaces(API)

Nowadays, API's are vividly used to pass data between different heterogeneous devices. These API's can be tampered creating a business loss to the organisation. To mitigate that we can encrypt the API Key and should be decrypted only at the server environment. Age limit should be set to these API keys and make users update their API Keys time-to-time. Real-Time API monitoring also helps to prevent the hacking of API.

D. Permanent Data Loss

Data in the cloud will be dynamic. These data should have a backup copy secured at different servers other than the running instance. This helps to restore the system state at the time of vulnerability. These backups are costly and the cost varies among providers. Maintaining a restricted set of users to perform activities in cloud environments helps to reduce the data attacks in the organisation.

V. Best Practises in Public Clouds

The security issues in public cloud services are increasing day-b-day[11]. 95% of the organizations are considering data security in public clouds. Here are few best practices to employ a secured and reliable cloud application in public clouds.

A. Access Management and Control

It is advised to provide access to a trusted and restricted set of users in the organisation. These access credentials should be timely changed to avoid data breaches. Email Triggers and Log Information should be recorded when an event happens with these credentials in the public service.

B. Vulnerability shielding

The Organisation must check the vulnerability of their cloud services utilized frequently. Timely updating the services reduce the risk of an attack of the cloud by the hackers[12]

C. Cloud Architecture

Cloud Architecture employs a major role in reducing attacks. Resources should be distributed and follow strict access control to unauthorized users. New Software / Packages updates for these resources should be properly inspected before updating. Resources should be properly managed to meet the organisation needs. Adaptation, run-time models, continuous development and deployment are some of the highly adopted principles to employ a better cloud architecture[13].

D. Data Backup

Data in the public cloud should be backed up safely to restore the system to a particular point. These Backups as aforementioned are costly and the cost varies from provider to provider. A best practice is to store the backup in a different server which is only accessed by restricted users. Some organisations prefer to save copies of data either in local or standalone computers.

E. Organisation Policies

Newly formed or established organisation must ensure that the employees are abiding with the data policies imposed and need to provide regular training on Data Importance, Case Study analysis which could mitigate future havoc.

VI. Conclusion

Cloud Computing is a revolutionized technology in the Information Technology Domain. These services are employed directly (or) indirectly by almost all IT organisations. Cloud services should be properly allocated and used. Newer Security concerns were constantly raised day-by-day in public clouds compared to other cloud delivery models. Effective practices should be lined up to keep the stored data safe from vulnerabilities. With the increase of attacks, we can't employ a one-stop solution to security challenges. The methods aforementioned will minimize threats to an extent. Reviewing the security policies and procedures helps to protect the data and its privacy.

Acknowledgment

We would like to thank Dr. Shajulin Benedict, Indian Institute of Information Technology Kottayam for supplying the conceptual knowledge during the research.

References

[1] A. Heydari, M. Tavakoli, and M. Riazi, "An overview of public cloud security issues," *International Journal of Management Excellence*, vol. 3, 06 2014.

[2] T. C. Group, "Cloud Computing and Security – A Natural Match," Tech. Rep., 04 2010.

[3] J. Sen, *Security and Privacy Issues in Cloud Computing*, 09 2013, vol. 3, pp. 1– 45.

[4] D. Teneyuca, "Internet cloud security: The illusion of inclusion," *Information Security Technical Report*, vol. 16, no. 3, pp. 102–107, 2011, cloud Security. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1363412711000501

[5] M. Ahmed and M. Hossain, "Cloud computing and security issues in the cloud," *International Journal of Network Security and Its Applications*, vol. 6, pp. 25–36, 01 2014.

[6] A. Yeang, Z. Zaaba, and N. Samsudin, "Reviews on security issues and challenges in cloud computing," *IOP Conference Series: Materials Science and Engineering*, vol. 160, p. 012106, 11 2016.

[7] N. Sehgal, Y. Xiong, W. Mulia, S. Sohoni, D. Fritz, and J. Acken, "A cross section of the issues and research activities related to both information security and cloud computing," *IETE Technical Review*, vol. 28, p. 279, 07 2011.

[8] K. S. S. Bulusu, "A study on cloud computing security challenges," Master's Thesis, Blekinge Institute of Technology, 2013.

[9] D. D. M. A. Viswanadham, "Security issues in cloud computing and associated mitigation techniques," *INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH TECHNOLOGY*, vol. 13, 2015.

[10] R. Jathanna and D. Jagli, "Cloud computing and security issues," *International Journal of Engineering Research and Applications*, vol. 07, pp. 31–38, 06 2017.

[11] P. Mell and T. Grance, "The nist definition of cloud computing," 2011-09-28 2011.

[12] Y. Z. An, Z. F. Zaaba, and N. F. Samsudin, "Reviews on security issues and challenges in cloud computing," *IOP Conference Series: Materials Science and Engineering*, vol. 160, p. 012106, nov 2016. [Online]. Available: https://doi.org/10.1088/1757-899x/160/1/012106

[13] C. Pahl, P. Jamshidi, and O. Zimmermann, "Architectural principles for cloud software," *ACM Transactions on Internet Technology*, vol. 18, 06 2017.