Risks in Cloud Computing

Abstract

Cloud computing is the delivery of services which includes servers, storage, databases, networking, software.In other words it's the on demand availability of computing resources as a service. It is looked upon as an alternate to the data centre which had to be present on premise earlier which in this case can be distributed over multiple locations in the web. This helps in providing easy access to all the required resources without having to be present on premise.
There are countless benefits of cloud computing which drives the option to move to the cloud. Few of them include increase in scalability produtivity accessibility while keeping minimal cost. But there are some vulnerabilities associated with it also. Some common risks include Loss of Data,Vendor Lock in,DOS attacks,Identity theft,privacy breach etc.In this paper we will look upon the common risks associated with cloud computing and discuss ways to minimise them.

Introduction

In this day and age cloud computing has become the platform of choice for many especially the customer-facing ones that need to scale dynamically.The worldwide cloud computing market is expected to grow to 191 billion dollar by 2020 from 91 billion dollar in 2015.
As more Businesses and governments are shifting more and more workloads to the cloud because of the benefits of cloud computing such as ubiquitous access, unlimited computational power and storage capacity, etc, at low cost, there has been more and more threats evolving in this field. So major concerns are arising about data security in cloud computing.

Problem Description

Some of the common risks regarding cloud computing are as follows:

Stolen Credentials

In case an attacker has found access to a user's cloud credentials, he can then the access CSP's services for additional resources in addition to target the organization's assets. He can also use the resources to target the organization's administrative users as well as other organizations using the same CSP.

Identity Theft

Identity theft is a tactic used by imposter who obtains key pieces of useful informations , such as driver's license number or PAN number to impersonate someone else.Here the attacker uses the stolen account information of the user to conduct malicious or unauthorized activity.

Denial of Service attack

Denial of service (DoS) attacks mostly happen when the attacker sends too much traffic to buffer the server. Generally,the attacker aims to disrupt the web servers of organizations like banking institutions, large media houses, and government sectors. After having the access to data those attacker try to negotiate with money to recover the lost data.

Vendor Lockin

Vendor lock-in is a general problem when an organization moves its operations from one CSP to another. This issue is more prominent in service models where the CSP has more responsibility. As an agency uses more features, services, or APIs, the CSP has to implement in a better way. These implementations require changes when moved to a different CSP. If a particular CSP shuts down because of failure in business, it becomes a major issue as data cannot be transferred to another CSP in a timely manner or can be complete lost.

Unauthorised Insider access

Staffs and network administrators who work as Insiders for both organizations and CSPs can exploit their position to access in an unauthorized manner which can lead to the organization's or CSP's networks, systems, and data to be damaged or valuable data exfiltrated.When using Infrastructure as a Service (IaaS) this is a serious issue as these unauthorised access can go undetected.

Loss of Data

There are few common ways which leads to loss of data. Overwriting data is the most common of the lot which happens when a data set are imported by numerous uploads.
Sometimes data is deleted accidentally which could be required by them later. Sometimes untrustworthy workers can also be the cause of loss of data.

Privacy Threat

Generally the data owners save their documents on to the servers along with the corresponding indices in encrypted form instead of plain text form to provide privacy to their data from the cloud service providers (CSPs). But the sensitive data can still be derived from the CSPs from the encrypted documents due to the data leak which are done after exploiting the vulnerabilities in the encrypted schemes.

Existing Work

There has been many ways devised to mitigate the vulnerabilities and minimise the risks.We have discussed few of them here. Companies must research the CSP carefully before using their services or even use the multi-cloud strategy so that they do not depend completely on a single CSP. They must ensure that their data is easily portable and can work with same efficiency on a different environment.Only service providers having proven records should be worked with. Encryption plays an important role in cloud data security.Practice to encrypt

network edge is used to ensure the movement of data is secure and not tampered.In addition to this data transmission endpoints should be authenticated

so that their legitimacy is confirmed. Multi-factor authentication plays a important role to diminish risks.In this case we combine a password with a secondary authentication component like PIN or OTP which adds an additional layer to the security.

Unannounced security tests should be run.In addition to that regular vulnerability test can be conducted.And based on the results they should evaluate the

major weaknesses and act accordingly. Employees can play a huge part in the unauthorised inside access. Therefore all the employees must be educated. There should be a basic plan set up for the employees to which everyone should adhere.Moreover background checks of the employees can be done to ensure no one is working having any malicious intent. Also changing of passwords on regular intervals must me done and employees must know how to create strong passwords firewalls are used block attackers IP address or the ports they are attacking. Sometimes this method may block the legitimate users also. Hence,intrusion detection system(IDS) comes into picture that prevents certain requests from reaching enterprise servers. As privacy of data is the main priority here, the company should actively and hugely invest on the tools which helps in maximising security. All the up- dates should be done regularly to make sure every security patch is up to date.

Companies should also use specific tools which sends simulated phishing emails to check how the employees behave in that given scenario. Lastly, they can keep internal backups of their data so that it is ready to host if is time consuming to extract it from the cloud or even if it fails.They should distribute data across multiple servers all over the globe and take backup daily.

Conclusion

In this internet age where everything is moving towards cloud and attackers are also getting smarter day by day.The above are some of the areas where innova- tion has been done and continues to be done.As this is a never ending process

we can never be sure that this will be risk free but its extremely important for the companies to devise ways to outsmart them and provide better security to the data of the customers.

References

[1] ScottPaquette, Paul T.Jaeger, Susan C.Wilson, Identifying the security risks associated with governmental use of cloud computing", Elsevier Government Information Quarterly, Volume 27, Issue 3, July 2010, Pages 245-253.
[2] Crouhy, M., Galai, D., Mark, R. (2006). The essentials of risk management. Toronto, ON: McGraw-Hill
[3] Bernstein, P. L. (1998). Against the gods: The remarkable story of risk. New York, NY: John Wiley Sons, Inc.
[4] Managing business risks in the information age. (1998). New York, NY: The Economist Intelligence Unit.
[5] Stoneburner, G., Goguen, A., Feringa, A. (2004). Risk management guide for information technology systems. Washington, DC.
[6] Straub, D., Welke, R. (1998). Coping with systems risk: security planning models for management decision making. MIS Quarterly, 22(4), 441469.
[7]Rashmi V. Deshmukh, Kailas K. Devadkar, Understanding DDoS Attack its Effect in Cloud Environment, Procedia Computer Science, Volume 49, 2015, Pages 202-210, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2015.04.245. (https://www.sciencedirect.com/science/article/pii/S1877050915007541)