Cloud Computing Technology: Security concern and Measure

[1]Vikas Yadav,[2]Amit Singh

vikasyadavmbd@gmail.com
amit84376@gmail.com

Abstract— **Cloud Computing is an on-demand or pay-as-you-go system of compute, networking, database, power, applications and other IT resources. In the cloud, many risks involved with data security. Storing data in the cloud might seem like a safe bet, and for most users it is. But risks will always exist. Below we have identified some serious security threats in cloud computing.**

Keywords— **Security, Risks, Cloud,Hijack,Encryption**

INTRODUCTION

The move to Cloud Computing brings with it a number of attributes that require special consideration when it comes to securing data. And since in nearly every organization, their most sensitive data will be stored either directly in a relational database, or ultimately in a relational database through an application, how these new risks impact database security in particular is worth considering. As users move applications involving sensitive data to the cloud, they need to be concerned with three key issues that affect database security:

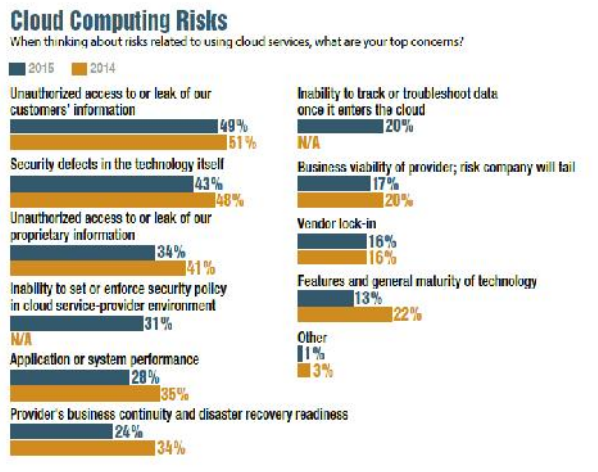
1) PRIVILEGED USER ACCESS– Sensitive data processed outside the enterprise brings with it an inherent level of risk, because outsourced services bypass the physical, logical and personnel controls IT departments exert over in-house programs. Put simply, outsiders are now insiders.

2) SERVER ELASTICITY – One of the major benefits of cloud computing is flexibility, so aside from the fact that you may not know (or could have little control over) exactly where your data is hosted, the servers hosting this data may also be provisioned and de-provisioned frequently to reflect current capacity requirements. This changing topology can be an obstacle to some technologies you rely on today, or a management nightmare if configurations must be updated with every change.

3) REGULATORY COMPLIANCE: Organizations are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. The ability to demonstrate to auditors that their data is secure despite a lack of physical control over systems, hinges in part on educating them, and in part on providing them with the necessary visibility into all activity.

IT firms are adopting and selling cloud services with abandon. Growth is over 100% for the past five years. While the cloud brings many benefits, many IT providers are aware of the risks in cloud computing and are charging ahead anyway.

This chart from an InformationWeek and Dark Reading survey shows the top cloud computing risks that concern IT professionals. As you can see, the top three center on the threat of unauthorized access and security.



I. DISTRIBUTED DENIAL OF SERVICE (DDOS) AND DENIAL OF SERVICE (DOS) ATTACKS

DDoS attacks are nothing new but can be especially crippling when targeted at your organization's public cloud. DDoS attacks often affect the availability and for enterprises that run critical infrastructure in the cloud. This type of attack can be debilitating, and systems may slow or time out.

DDoS attacks also consume significant amounts of processing power – a bill that the cloud customer (you) will have to pay.

II. LACK OF EXPERTISE:

With the quick advancements and improvements in cloud technologies, more and more organizations are clouds to place their workloads. However, they face difficulties to keep up with the tools which require particular expertise. Organizations can deal with this challenge by providing cloud technologies training to their sys admins along with development staff.

III. RISKS RELATED TO LACK OF CONTROL

When you host and maintain a service on a local network, then you have complete control over the features you choose to use. If you want to change the service in the future, you are in control.

However, when you use a cloud service provider, the vendor is in control. You have no guarantee that the features you use today will be provided for the same price tomorrow. The vendor can double its price, and if your clients are depending on that service, then you might be forced to pay.

Also, who controls access to your data in a cloud service? What happens if you are not able to make payment?

IV. WEAK AUTHENTICATION AND IDENTITY MANAGEMENT

A lack of proper authentication and identity management is responsible for data breaches within organizations. Businesses often struggle with identity management as they try to allocate permissions appropriate to every user's job role. For example, the Anthem Inc. data breach resulted in cyber-criminals accessing 80 million records containing personal and medical information. This hack was the result of stolen user credentials; Anthem had failed to deploy multi-factor authentication.

Poor identity management can leave gaping holes in enterprise cyber-security. Two-factor/Multi-factor authentication systems, like one-time passwords and phone-based authentication, protect cloud services by making it harder for attackers to log in using stolen passwords. This is a preventative discussion that every business that has an online presence should have to ensure the safety of its customers.

V. LACK OF EXPERTISE:

With the quick advancements and improvements in cloud technologies, more and more organizations are clouds to place their workloads. However, they face difficulties to keep up with the tools which require particular expertise. Organizations can deal with this challenge by providing cloud technologies training to their sys admins along with development staff.

By adding cloud specialists to IT teams may be costly too for small and medium businesses (SMBs). Luckily, various routine activities that specialists perform can be automated using automated tools. Now, many organizations are also moving to DevOps tools, like Puppet and Chef due to their multi-tasking and automation capabilities such as monitoring resource usage, automating backups etc. These automating tools considerably contribute to cloud optimization for cost, security, and governance.

VI. SECURITY RISKS AT THE VENDOR

When a cloud service vendor supplies a critical service for your business and stores critical data – such as customer payment data and your mailing lists – you place the life of your business in the vendor's hands.

Ask yourself – how clean are those hands?Many small businesses know almost nothing about the

people and technology behind the cloud services they use.

They rarely consider:

1. The character of the vendor's employees
2. The security of the vendor's technology
3. The access the vendor has to their data

When you depend on a cloud service for a business-critical task, then you put the trust of your business into the hands of other people and the quality of their work.

Your reputation no longer depends on the integrity of only your business – now it also depends on the integrity of the vendor's business. And that's a cloud computing risk.

Even if you know the number of people at a vendor who can access your data, how well do you know each person? Can you trust them with the reputation of your company?

VII. Lacking or Insufficient Due Diligence

Due diligence is the process of evaluating cloud vendors to ensure that best practices are in place. Part of this process includes verifying whether the cloud provider can offer adequate cloud security controls and meet the level of service expected by an enterprise.

"Too many enterprises jump into the cloud without understanding the full scope of the undertaking," said the report. Without an understanding of the service providers' environment and protections, customers don't know what to expect in the way of incident response, encryption use, and security monitoring. Not knowing these factors means "organizations are taking on unknown levels of risk in ways they may not even comprehend, but that are a far departure from their current risks," wrote the authors.

Chances are, expectations will be misaligned between customer and service. What are the contractual obligations for each party? How will liability be divided? How much transparency can a customer expect from the provider in the face of an incident?

Enterprises may push applications that have both internal on-premises network security controls and in the cloud, when network security controls fail and don't work. If enterprise architects don't understand the cloud environment, their application designs may not function with appropriately.

VIII. Data Security:

CSPs are responsible to provide clouds' security, but they're not responsible for your apps, servers, and security of data. As per CDW 2013 State of the Cloud Report, "46 percent of respondents face security of data or applications as a significant challenge."

When your CSP ensure you about the complete compliance and regulation, don't consider it as 100% compliant and yielding. You still require to encrypt and secure your own data and should invest in buying suite of tools from your CSP to protect your data from cyber-attacks.

Following questions may be asked before engaging with your cloud service provider.

- Can you ensure protection of my data?
- How will you protect my data from corruption?
- Do you have experts and professionals on board if something happens wrong?

IX. Unauthorized access to customer and business data

Criminals do not like to work. They may target small business networks because they are easier to breach, and they often go after larger companies because of the allure of larger payouts.

Cloud services aggregate data from thousands of small businesses. The small businesses believe they are pushing security risks to a larger organization more capable of protecting their data.

However, each business that uses a cloud service increases the value of that service as a potential target. This concentrates risk on a single point of failure. A disaster at a cloud provider can affect every one of its customers.

And hackers and malware are not the only ones who may target a cloud service provider. Cloud computing risks are also presented by insider threats.

Once you outsource a service to a third-party server, you now have to worry about your staff and the vendor's staff. More people have access to the data and systems that support the service, which means you have to extend trust to people you have never met.

The risk of government intrusion also increases when you use a cloud service. Ask yourself, if Uncle Sam more likely to snoop on your email server or an email server used by a hundred companies and maintained by Microsoft?

X. Weak authentication and identity management

A lack of proper authentication and identity management is responsible for data breaches within organizations. Businesses often struggle with identity management as they try to allocate permissions appropriate to every user's job role. For example, the Anthem Inc. data breach resulted in cyber-criminals accessing 80 million records containing personal and medical information. This hack was the result of stolen user credentials; Anthem had failed to deploy multi-factor authentication.

Poor identity management can leave gaping holes in enterprise cyber-security. Two-factor/Multi-factor authentication systems, like one-time passwords and phone-based authentication, protect cloud services by making it harder for attackers to log in using stolen passwords. This is a preventative discussion that every business that has an online presence should have to ensure the safety of its customers.

XI. Cloud Migration

Cloud migration is the process of moving data, applications, and other important information of an organization from its on-premises either desktops or servers to the cloud infrastructure, and this can also involve in moving data between different cloud setups.

Cloud migration enables all the computing capabilities those were performed earlier by devices installed on-premises. Cloud migration is a big challenge as many companies when they require to migrate from on-premises to cloud or from one cloud to another, they partner with experienced cloud service provider.

XII. Compliance and legal risks

Are you in an industry that regulates data security? The list includes healthcare, banking, government, and anyone that accepts credit cards – and the list of regulated industries continues to grow.

Many data security regulations are intended to protect a specific type of data. For example, HIPAA requires healthcare providers to protect patient data. PCI DSS requires anyone who accepts credit cards to protect cardholder data.

Not only are the companies covered by these regulations required to protect the data, they are also typically required to know

Where the data resides

Who is allowed to access it

How it is protected

If a company outsources the processing or storage of data that it is required to protect, then it is relying on a cloud service provider to maintain their compliance.

If the company does not have adequate legal protections, then it may be liable when there is a data breach at the cloud service that exposes the company's data.

In other words, unless you are protected in writing, then a cloud service provider might not be liable for a breach of your data on its systems. So you are transferring the responsibility of protecting the data to a third party, but you are still liable if that party fails to live up to the task.

This is one of the many risks in cloud computing. Even if a vendor has your best interests at heart, your interests will always be secondary to theirs.

XIII. Abusing Cloud Services -- Especially Infrastructure

Cloud computing brings large-scale, elastic services to enterprise users and hackers alike. The lower cost of deploying infrastructure means that carrying out an attack is trivial, from a cost perspective. "It might take an attacker years to crack an encryption key using a limited hardware.

But using an array of cloud servers, he might be able to compromise it in minutes," the report noted. Or hackers might use cloud servers to serve malware, launch DDoS attacks, or distribute pirated software.

Responsibility for the use of cloud services rests with service providers, but how will they detect inappropriate uses? Do they have clear definitions of what constitutes abuse? How will it be prevented in the future if it occurs once? The report left resolution of the issue up in the air. Cloud customers will need to assess service provider behavior to see how effectively they respond.

XIV. Availability risks

No service can guarantee 100% uptime. When you rely on a cloud service for a business-critical task, then you are putting the viability of your business in the hands of two services: the cloud vendor and your ISP.

If your internet access goes down, then it will take your vendor's cloud service with it. If you need the cloud service to process customer payments or access important data, too bad – you have to wait until the internet is back up.

Another cloud risk is that the vendor can go down as well. Anything from bad weather, DDoS attacks, or a good ol' system failure can knock the service unresponsive.

How much uptime can your cloud vendor provide? 99%? That's great, but consider that statistic for a moment….

99% uptime means 1% downtime. Over the course of 365 days, that's 3.65 days the service will be down. That's equal to 87.6 hours.

But when do those hours occur? Late at night? During the day?

If those 87 hours were to occur during business hours, then that's equivalent to 10 days of downtime.

Can your client live without this service for 10 business days?

And remember: That's just for the cloud service. The client's internet connection will also experience downtime. If you again assume 99% uptime and 1% downtime, then that's as much as 20 business days that your client will not be able to reach the cloud service.

Can your client live without the service for 20 days?

XV. Data Breaches

Cloud data storage and cloud computing, in general, have forced cyber-criminals to invent new ways to circumvent security technology so they can administer their new methods of attack.

It's every CIO's worst nightmare: standing in front of an endless row of cameras and provide an embarrassing assessment of the situation. Along with the legal requirements, comes full disclosure and potential lawsuits, similar to the recent incident with Equifax.

Although cloud storage providers implement rigorous security measures, the same threats that impact traditional storage networks also threaten the cloud world. A data breach can expose sensitive customer information, intellectual property, and trade secrets, all of which can lead to serious consequences. For example, companies could face lawsuits and hefty fines as well as damage to the brand image that could last for years.

It's possible for a user on one virtual machine to listen for activity that signals the arrival of an encryption key on another VM on the same host. It's called the "side channel timing exposure," resulting in the organization's sensitive internal data falls into the hands of their competitors.

Reputable cloud services usually have several security protocols in place to protect confidential information. However, it's up to your organization to implement a plan for protecting your data in the cloud. The most efficient method is to use encryption and multi-factor authentication.

If sensitive or regulated data is put in the cloud and a breach occurs, the company may be required to disclose the breach and send notifications to potential victims. Certain regulations such as HIPAA and HITECH in the healthcare industry and

the EU Data Protection Directive require these disclosures. Following legally-mandated breach disclosures, regulators can levy fines against a company, and it's not uncommon for consumers whose data was compromised to file lawsuits.

XVI. INCOMPATIBILITY:

During moving workloads from on-premises to the cloud, the common issue the incompatibility between on-premises infrastructure and the services which are companies going to buy from the public cloud providers. In last current years, most CSPs tried to create "connectors of sort" to make practices more standardize and homogenous.

XVII. DOWNTIME:

Businesses suppose complete data accessibility and availability when their data is stored on cloud anytime from anywhere. The main challenge most organizations face is they can access their data from cloud only through internet connection. So, poor internet connection can disrupt cloud services and higher risks of data accessibility.

XVIII. BANDWIDTH COST:

Though organizations and businesses can save money on hardware using cloud, but they have to pay extra for the bandwidth they use to access their workloads. However, it doesn't charge much for smaller apps, but data-intensive apps need more bandwidth which can costs higher.

XIX. MALICIOUS INSIDERS

With the Edward Snowden case and NSA revelations in the headlines, malicious insiders might seem to be a common threat. If one exists inside a giant cloud organization, the hazards are magnified. One tactic cloud customers should use to protect themselves is to keep their encryption keys on the premises, not in the cloud.

"If the keys are not kept with the customer and are only available at data-usage time, the system is still vulnerable to a malicious insider attack." Systems that depend "solely on the cloud service provider for security are at great risk" from a malicious insider, the report said

XX. DATA LOSS

A data breach is the result of a malicious and probably intrusive action. Data loss may occur when a disk drive dies without its owner having created a backup. Data loss happens when the owner of encrypted data loses the key that unlocks it. Small amounts of data were lost for some Amazon Web Service customers as its EC2 cloud suffered "a re-mirroring storm" due to human operator error on Easter weekend in 2011. And a data loss could occur intentionally in the event of a malicious attack.

Although the chances of losing all your data in the cloud are minimal, there have been some reports of hackers gaining access to cloud data centers and wiping all the data clean. That's why it's important to distribute your applications across several zones and backup your data using off-site storage when possible.

You also need to be aware of compliance policies that govern what you can and can't do with collected data. Understanding these rules will protect you in the event of a data breach and keep you away from trouble.

tems one and two usually lead to a loss of customer confidence. When the public does not trust how you handle data, they take their business elsewhere resulting in lower revenue.

XXI. HIJACKED ACCOUNTS - COMPROMISED CREDENTIALS

Account hijacking sounds too elementary to be a concern in the cloud, but Cloud Security Alliance says it is a problem. Phishing, exploitation of software vulnerabilities such as buffer overflow attacks, and loss of passwords and credentials can all lead to the loss of control over a user account. An intruder with control over a user account can eavesdrop on transactions, manipulate data, provide false and business-damaging responses to customers, and redirect customers to a competitor's site or inappropriate sites. Even worse, if the compromised account is connected to other

accounts, you can quickly lose control of multiple accounts.

You'd be surprised how many security threats can be prevented by just choosing a secure, unique password per account. Remembering these passwords can be a challenge, so use a trusted password manager. Companies that don't stress the importance of secure credentials are at a greater risk of being compromised. In addition to using strong passwords, companies can also protect themselves by setting the right user roles and creating processes for identifying critical changes made by other users

XXII. Hacked Interfaces and Insecure APIs

The cloud era has brought about the contradiction of trying to make services available to millions while limiting any damage all these mostly anonymous users might do to the service. The answer has been a public facing application programming interface, or API, that defines how a third party connects an application to the service.

Most cloud services and applications use APIs to communicate with other cloud services. As a result, the security of the APIs themselves has a direct effect on the security of the cloud services. The chance of getting hacked increases when companies grant third parties access to the APIs. In a worst-case scenario, this could cause the business to lose confidential information related to their customers and other parties.

According to the CSA, the best way to protect yourself from API hacks is to implement threat modeling applications and systems into the development lifecycle. It's also recommended that you perform thorough code reviews to ensure that there aren't any gaps in your security.

Conclusion

We've discussed cloud computing risks at some length, so it's helpful to remember *what* is at risk.

A breach of your data or your client's data can be devastating depending on the type of data and the extent of the breach.

The costs of investigating and resolving a breach, associated legal expenses, and the losses to a company's reputation, can be enough to shut its doors.

The risks related to the availability of a cloud service are less severe, but still damaging.

Depending on the nature of the service and its importance to your day-to-day operations, an outage can mean anything from a temporary headache to a massive disruption that costs the company thousands.

Is cloud computing worth the risk? It's up to you to decide.

References

[1] S.Tanvi, Ambuj Kr Agarwal, and S. K. Singh. "Study of Cloud Computing and its Security Approaches."

[2] Saxena, Ashendra Kr, Ambuj Kr Agarwal, and Danish Ather. "HOW TO SECURE DESIGN USING THREAT MODELING."

[3] Agarwal, Ambuj Kumar, and Vinodani Katiyar. "A Study of Software Matrix Systems: A Comparative Study of existing Software Matrix Systems."

[4] Saleem, Ambreen, and Ambuj Kumar Agarwal. "Analysis and Design of Secure Web Services." Proceedings of Fifth International Conference on Soft Computing for Problem Solving. Springer Singapore, 2016.

[5] S. Fatima, A. Agarwal and P. Gupta, "Different approaches to convert speech into sign language," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2016, pp. 180-183.

[6] S. Shukla, A. K. Agarwal and A. Lakhmani, "MICROCHIPS: A leading innovation in medicine," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2016, pp. 205-210.

[7] D. Sehgal and A. K. Agarwal, "Sentiment analysis of big data applications using Twitter Data with the help of HADOOP framework," 2016 International Conference System Modeling & Advancement in Research Trends (SMART), Moradabad, 2016, pp. 251-255.doi:10.1109/SYSMART.2016.7894530
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7894530&isnumber=7894471

[8] https://www.myvirtualjourney.com/challenges-and-risks-in-cloud-computing/

[9] https://www.datapine.com/dashboard-examples-and-templates/market-research

[10] https://public.datapine.com/?&_ga=2.255695502.74577456.1551252068-1234997213.1551252068#board/BKAnfWTeuauadZD9G3gv9L