Major Cloud Computing Security Challenges and New Algorithms for Protection

[1]Mercy Deepa A, [2]Benitsha A, [3]Daniel Silvanus P, [4]Ganesan A.

[1,2,3]Student, [4]Associate Professor, Hindusthan College of arts and science, Coimbatore India,

[1]deepamercy33@gmail.com

Abstract Cloud computing is one of today's most exciting technologies due to its ability to reduce costs associated with computing while increasing flexibility and scalability for computer processes. During the past few years, cloud computing has grown from being a promising business idea to one of the fastest growing parts of the IT industry. IT organizations have expresses concern about critical issues (such as security) that exist with the widespread implementation of cloud computing. These types of concerns originate from the fact that data is stored remotely from the customer's location; in fact, it can be stored at any location. Security, in particular, is one of the most argued-about issues in the cloud computing field; several enterprises look at cloud computing warily due to projected security risks. The risks of compromised security and privacy may be lower overall, however, with cloud computing than they would be if the data were to be stored on individual machines instead of in a so - called "cloud" (the network of computers used for remote storage and maintenance). Comparison of the benefits and risks of cloud computing with those of the status quo are necessary for a full evaluation of the viability of cloud computing. Consequently, some issues arise those clients need to consider as they contemplate moving to cloud computing for their businesses. In this paper I summarize reliability, availability, and security issues for cloud computing (RAS issues), and propose feasible and available solutions for some of them.

Keywords —Cloud, Security, Breaches, Challenges, Network, Computing, Machine Learning, Logistic Regression

I. INTRODUCTION

Cloud security, also known as cloud computing security, consists of a set of policies, controls, procedures and technologies that work together to protect cloud-based systems, data, and infrastructure. These security measures are configured to protect cloud data, support regulatory compliance and protect customers' privacy as well as setting authentication rules for individual users and devices. From authenticating access to filtering traffic, cloud security can be configured to the exact needs of the business. And because these rules can be configured and managed in one place, administration overheads are reduced and IT teams empowered to focus on other areas of the business.

Cloud computing is on-demand access, via the internet, to computing resources—applications, servers (physical servers and virtual servers), data storage, development tools, networking capabilities, and more—hosted at a remote data center managed by a cloud services provider (or CSP). The CSP makes these resources available for a monthly subscription fee or bills them according to usage.

II. CHARACTERISTICS

On-demand self-services: The Cloud computing services does not require any human administrators, user themselves are able to provision, monitor and manage computing resources as needed.

Broad network access: The Computing services are generally provided over standard networks and heterogeneous devices.

Rapid elasticity: The Computing services should have IT resources that are able to scale out and in quickly and on as needed basis. Whenever the user require services it is provided to him and it is scale out as soon as its requirement gets over.

Resource pooling: The IT resource (e.g., networks, servers, storage, applications, and services) present are shared across multiple applications and occupant in an uncommitted manner. Multiple clients are provided service from a same physical resource.

Measured service: The resource utilization is tracked for each application and occupant, it will provide both the user and the resource provider with an account of what has been

 DOI : 10.35291/2454-9150.2022.0170

used. This is done for various reasons like monitoring billing and effective use of resource.

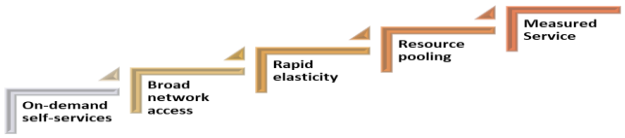

Fig 1:Cloud Computing Characteristic Features

III. INFRASTRUCTURE

Cloud infrastructure consists of servers, storage devices, network, cloud management software, deployment software, and platform virtualization.

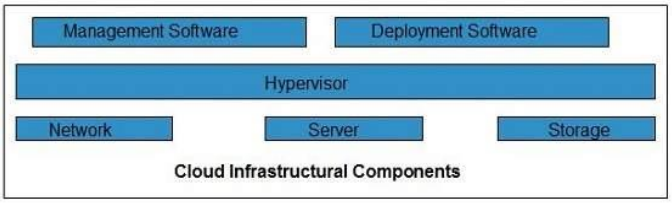

Fig 2: Components of Infrastructure

a. Hypervisor

Hypervisor is a **firmware** or **low-level program** that acts as a Virtual Machine Manager. It allows to share the single physical instance of cloud resources between several tenants.

b. Management Software

It helps to maintain and configure the infrastructure.

c. Deployment Software

It helps to deploy and integrate the application on the cloud.

d. Network

It is the key component of cloud infrastructure. It allows to connect cloud services over the Internet. It is also possible to deliver network as a utility over the Internet, which means, the customer can customize the network route and protocol.

e. Server

The **server** helps to compute the resource sharing and offers other services such as resource allocation and de-allocation, monitoring the resources, providing security etc.

f. Storage

Cloud keeps multiple replicas of storage. If one of the storage resources fails, then it can be extracted from another one, which makes cloud computing more reliable.

IV. CONSTRAINTS

Fundamental constraints that cloud infrastructure should implement are shown in the following diagram:

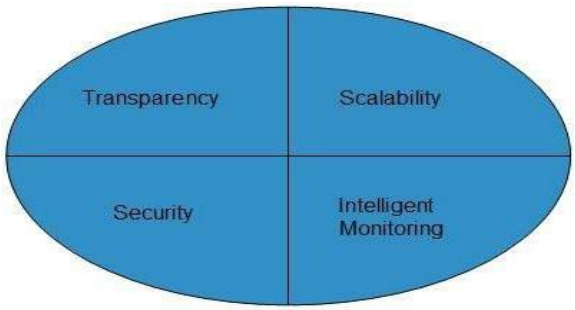

Fig 3: Constraints for Implementation

a) Transparency

Virtualization is the key to share resources in cloud environment. But it is not possible to satisfy the demand with single resource or server. Therefore, there must be transparency in resources, load balancing and application, so that we can scale them on demand.

b) Scalability

Scaling up an application delivery solution is not that easy as scaling up an application because it involves configuration overhead or even re-architecting the network. So, application delivery solution is need to be scalable which will require the virtual infrastructure such that resource can be provisioned and de-provisioned easily.

c) Intelligent Monitoring

To achieve transparency and scalability, application solution delivery will need to be capable of intelligent monitoring.

d) Security

The mega data center in the cloud should be securely architected. Also the control node, an entry point in mega data center, also needs to be secure.

V. IMPORTANCE OF SECURITY

Cloud security offers many benefits, including:

1. **Centralized security**: Just as cloud computing centralizes applications and data, cloud security centralizes protection. Cloud-based business networks consist of numerous devices and endpoints that can be difficult to manage when dealing with shadow IT or BYOD. Managing these entities centrally enhances traffic analysis and web filtering, streamlines the monitoring of network events and results in fewer software and policy updates. Disaster recovery plans can also be implemented and actioned easily when they are managed in one place.

2. **Reduced costs**: One of the benefits of utilizing cloud storage and security is that it eliminates the need to invest in dedicated hardware. Not only does this reduce capital expenditure, but it also reduces

 DOI : 10.35291/2454-9150.2022.0170

administrative overheads. Where once IT teams were firefighting security issues reactively, cloud security delivers proactive security features that offer protection 24/7 with little or no human intervention.

3. **Reduced Administration**: When you choose a reputable cloud services provider or cloud security platform, you can kiss goodbye to manual security configurations and almost constant security updates. These tasks can have a massive drain on resources, but when you move them to the cloud, all security administration happens in one place and is fully managed on your behalf.

4. **Reliability**: Cloud computing services offer the ultimate in dependability. With the right cloud security measures in place, users can safely access data and applications within the cloud no matter where they are or what device they are using.

Fig 4: Security Importance

VI. CHALLENGES AND SOLUTIONS

According to the 2020 Cloud Security Report, the highest ranking threat was misconfiguration, with 68% of companies citing this as their greatest concern (up from 62% from the previous year). Misconfiguration takes place when a cloud-related system, tool, or asset is not configured properly, thus endangering the system and exposing it to a potential attack or data leak. This threat was followed by unauthorized access (58%), insecure interfaces (52%), and account hijacking (50%). As powerful and innovative as the cloud is, it's also complex and ever changing. From a security standpoint, this creates lots of challenges, and loopholes.Cloud technology turned cybersecurity on its head. The availability and scope of data, and its interconnectedness, also made it extremely vulnerable to many threats. And it took a while for companies to take this issue seriously.

The transition to the cloud has brought new security challenges. Since cloud computing services are available online, this means anyone with the right credentials can access it. The availability of enterprise data attracts many hackers who attempt to study the systems, find flaws in them, and exploit them for their benefit. One of the main problems that come with assessing the security risks of cloud computing is understanding the consequences of letting these things happen within your system.

Fig 5: Security Challenges

1.DDoS and Denial-of-Service Attacks

A DDoS or distributed denial-of-service attack is a malicious attempt by hackers to disrupt the normal operations of your service or network by overwhelming your server with a flood of traffic. The goal is to make your server unavailable to its intended users, thereby disrupting operations (and your business). A successful attack can cause hours (or even days) of downtime, which can result in loss of revenue and customer trust.

SOLUTIONS

a. **Detect:** To prevent a distributed attack, your security service has to be able to distinguish between a high volume of real traffic and an actual attack.

b. **Respond:** When an attack is detected, your security network will respond by throttling malicious bot traffic while leaving normal traffic alone.

c. **Route:** To prevent a denial of service, your network needs to intelligently route the traffic into manageable chunks to avoid overwhelming your servers.

d. **Adapt:** Your security network should improve over time as it identifies and adapts to attack patterns.

2. Data loss

When business critical information is moved into the cloud, it's understandable to be concerned with its security. Losing cloud data, either through accidental deletion and human error, malicious tampering including the installation of malware (i.e. DDoS), or an act of nature that brings down a cloud service provider, could be disastrous for an enterprise business. Often a DDoS attack is only a diversion for a greater threat, such as an attempt to steal or delete data.

 DOI : 10.35291/2454-9150.2022.0170

Obviously, maintaining access to your data and keeping it safe at every level is crucial. That is why it is important to implement a robust data loss prevention (DLP) plan as part of your cloud security strategy.

SOLUTIONS

a. Backup, backup, backup

The number-one way to prevent data loss is to regularly back it up so you have a way to retrieve or recover it in the event of loss or leakage.

b. Use DLP software

With this software, you can automate your backup and loss prevention processes so your security measures don't fall through the cracks.

c. Perform a risk assessment

Audit your data to discover where and how your data is stored on the cloud. Once you have an inventory of your data storage, create a data flow map to understand your data processes and identify potential vulnerabilities.

A. 3. Concurrence violations

Concurrence is one of the biggest obstacles many organizations face when deciding whether to adopt cloud-based operations. Regulatory controls focus heavily on cloud security, and Concurrence violations can have a significant negative impact on your business and bottom line (including potentially heavy fines, and even lawsuits).

SOLUTIONS

a. Operational consistency and clarity

As you move into the cloud, it's important to migrate your operational processes smoothly into the cloud environment. The more consistent you are in your cloud operations and management, the easier it is to recognize and correct security issues (as well as other non-compliant areas) and respond to audits with accurate reporting.

b. Data visibility and security

Before the cloud, it was easy to locate your data in the data center. Now, data is spread across servers and an increasingly mobile and distributed workforce. This introduces challenges for organizations that must comply with strict data residency regulations in a global market. Getting a clear picture of your data is increasingly important and increasingly difficult. In addition, the more distributed your data (especially across unofficial servers and applications, also known as Shadow IT), the greater the threat to your data security.

c. Concurrence responsibility

Another challenge of security and Concurrence is determining who is actually responsible for ensuring you meet those requirements. The level of service and the cloud provider you choose will affect what responsibility you have to meet compliance regulations and how much your service provider will manage compliance for you. Clarifying these roles and ensuring there are no gaps in your compliance strategy and processes is critical for making sure you meet all regulations.

4. Data Breaches

A data breach is when confidential information is accessed and extracted without authorization. It affects the impact to reputation and trust of customers or partners. Loss of intellectual property (IP) to competitors, which may effect products release. Regulatory implications that may result in monetary loss.

Legal, contractual liabilities and financial expenses incurred due to incident response and forensics.

SOLUTIONS

a. Apply the Principle of Least Privilege (PoLP)

Least Privilege is the practice of restricting access rights for users, accounts, systems, and processes to only the minimum resources needed to perform routine tasks and duties. In other words, users (e.g., employees) are given the lowest clearance level needed to perform their job.

The goal is to reduce the risk of security breaches by limiting access to only those who need it. Forrester Research estimates that 80% of security breaches involve the theft of privileged credentials. By implementing least privilege policy, organizations can significantly reduce opportunities for exploitation, limit the fallout from a breach, and improve compliance across the network.

b. Use multi-factor authentication

Multi-factor authentication (MFA) is a security method for logins that requires two or more credentials from a user to confirm their identity before granting access. This is a simple but effective way to more tightly secure your data and strengthen your access points against potential hackers.

c. Encrypt data at rest

Data is at rest when it is not actively used and is stored on a hard drive. While these data are usually protected by basic perimeter defenses like firewalls, encrypting your hard drives (and other data at rest) adds another layer of protection.

5. Notifications and alerts

Awareness and proper communication of security threats is a cornerstone of network security and the same goes for cloud computing security. Alerting the appropriate website or application managers as soon as a threat is identified should be part of a thorough data security and access management plan. Speedy mitigation of a threat relies on

 DOI : 10.35291/2454-9150.2022.0170

clear and prompt communication so steps can be taken by the proper entities and impact of the threat minimized.

SOLUTIONS

a. Automate security notifications and alerts

When it comes to security, automation is your friend. Operating on the cloud provides numerous opportunities to implement automation that will increase efficiency and reduce human error.

As you build out your cloud security strategy, be sure to include automated security alerts and notifications in your processes. An automated security notification system will alert you in real time to potential or immediate threats, including attacks, vulnerabilities, and even gaps in your compliance.

6. Account Hijacking

Many people have extremely weak password security, including password reuse and the use of weak passwords. This problem exacerbates the impact of phishing attacks and data breaches since it enables a single stolen password to be used on multiple different accounts. Account hijacking is one of the more serious cloud security issues as organizations are increasingly reliant on cloud-based infrastructure and applications for core business functions.

An attacker with an employee's credentials can access sensitive data or functionality, and compromised customer credentials give full control over their online account. Account hijacking is a threat in which malicious attackers gain access to and abuse accounts that are highly privileged or sensitive. In cloud environments, the accounts with the highest risks are cloud service accounts or subscriptions.

SOLUTIONS

1) Implement strong access controls and procedures

While vulnerabilities within the technology itself are a serious concern, a huge risk to your data security comes from your human resources. Lax access controls and procedures make it easy for hackers to sneak into your systems and wreak havoc. Create strong procedures for access management (including multi-factor authentication and least privilege) to minimize risk around access points.

7. Cyberattacks

Cybercrime is a business, and cybercriminals select their targets based upon the expected profitability of their attacks. Cloud-based infrastructure is directly accessible from the public Internet, is often improperly secured, and contains a great deal of sensitive and valuable data. Additionally, the cloud is used by many different companies, meaning that a successful attack can likely be repeated many times with a high probability of success. As a result, organizations' cloud deployments are a common target of cyberattacks.

SOLUTIONS

a) Identity theft, fraud, extortion

b) Malware, phishing, spamming, spoofing, spyware, trojans and viruses

c) Stolen hardware, such as laptops or mobile devices

d) Denial-of-service and distributed denial-of-service attacks

e) Breach of access

f) Password sniffing

g) System infiltration

h) Website defacement

i) Private and public Web browser exploits

j) Instant messaging abuse

k) Intellectual property (IP) theft or unauthorized

l) access

CYBER BREACHES

	Num	Name_of_Covered_Entity	State	Business_Associate_Involved	Individuals_Affected	Date_of_Breach	Type_of_Breach
1	0	Brooke Army Medical Center	TX	Democracy Data & Communications, LLC (	1000	10/16/2009	Theft
2	1	Mid America Kidney Stone Association, LLC	MO	Blue Cross Blue Shield of RI	1000	9/22/2009	Theft

 DOI : 10.35291/2454-9150.2022.0170

3	2	Alaska Department of Health and Social Services	AK	Rick Lawson,	501	11/26/2013	Theft
4	3	Health Services for Children with Special Needs, Inc.	DC	Health Behavior Innovations (HBI)	3800	12/30/2013	Loss
5	4	L. Douglas Carlson, M.D.	CA	Professional Computer Services	5257	9/27/2009	Theft
6	5	David I. Cohen, MD	CA	MSO of Puerto Rico, Inc.	857	9/27/2009	Theft
7	6	Michele Del Vicario, MD	CA	MSO of Puerto Rico	6145	9/27/2009	Theft

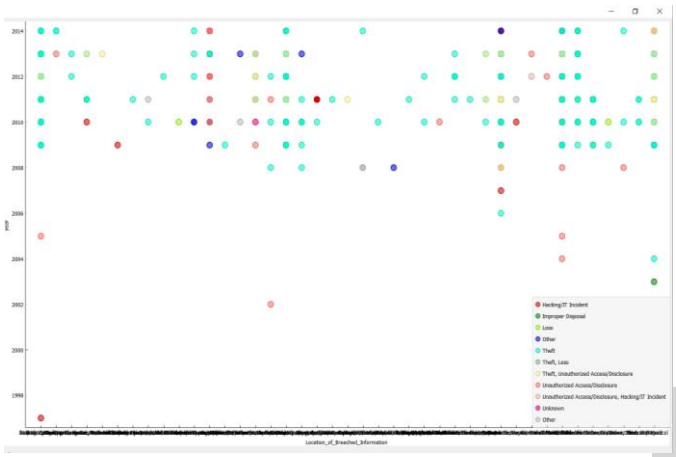

FIG 6: COMPARISON OF CYCBER SECURITY BREACHES

CONCLUSION

Doubtless, Cloud computing helps IT enterprises use various techniques to optimize and secure application performance in a cost-effective manner. Additionally, just because the software can run in a Virtual machine does not mean that it performs well in cloud environment necessarily. Thereupon, in cloud there are risks and hidden costs in managing cloud compliance. The key to successful cloud computing initiatives is achieving a balance between the business benefits and the hidden potential risks which can impact efficacy. Cloud providers often have several powerful servers and resources in order to provide appropriate services for their users but cloud is at risk similar to other Internet-based technology. In the other hand, they are also at risk of attacks such as powerful DDoS attacks similar other Internet-based technology.

As a solution, cloud providers can add more resource to protect themselves from such attacks but unfortunately there is no defense against a powerful DDoS attack which has good sapience. These issues which discussed in this paper are the main reasons that cause many enterprises which have a plane to migrate to cloud prefer using cloud for less sensitive data and store important data in their own local machines. Eventually, Whilst Cloud computing is an applicable an? interesting technology that introduce in the IT industry; It doesn't mean that all business IT needs to move to cloud. In addition, As a result, Moving toward cloud computing require to consider several parameters and most important of them is security.

REFERENCES

[1] Ashkan Paya and Dan C. Marinescu:, “Energy-aware Load Balancing and Application Scaling for the Cloud Ecosystem”, IEEE 2015. International Journal of Science, Engineering and Technology Research (IJSET)

[2] ClaudioFiandrino, Dzmitry Kliazovich, Pascal Bouvry Albert Y. Zomaya, “Performance and Energy Efficiency Metrics for Communication Systems of Cloud Computing Data Centers”, IEEE 2015.

[3] Guo Bing, Shen Yan, and Shao ZL, "The Redefinition and Some Discussion of Green Computing", Chinese Journal of Computers, vol. 32, Dec. 2009, pp. 2311-2319.

[4] IEEE Standard 1680-IEEE Standard for Environmental Assessment of Personal Computer Products, Including Laptop Personal Computers, Desktop Personal Computers, and Personal Computer Monitors.Standards Activities Board of the IEEE Computer Society.2006.

[5] J. C. Xu, “Current Situation and Countermeasures of Energy Conservation and Emission Reduction in Telecommunication Industry in China,” Modern Economic Information, vol. 7, p. 304, 2014.

[6] Jiaxin Li , Dongsheng Li, Yuming Ye, and Xicheng Lu, “Efficient Multi-Tenant Virtual Machine Allocation in Cloud Data Centers”, IEEE 2015

[7] Jinn-Tsong Tsai Jia-Cen Fang, Jyh-Horng Chou “Optimized task scheduling and resource allocation on cloud computing environment uses Improved Differential Evolution Algorithm (IDEA)”, Science Direct 2014.

[8] Mehiar Dabbagh, Bechir Hamdaoui, Mohsen Guizani, Ammar Rayes, “Towards Energy-Efficient Cloud Computing: Prediction, Consolidation, and Over commitment”, IEEE 2015.

[9] Mydhili K Nair, Dr.V.Gopalakrishna, "Generic Web Services: A Step Towards Green Computing", International Journal on Computer Science and Engineering, Vol.1, Mar. 2009, pp. 248-253.

[10] Sergi Figuerola, Mathieu Lemay, Victor Reijs, Michel Savoie, Bill St.Arnaud, "Converged Optical Network Infrastructures in Support of Future Internet and Grid Services using IaaS to Reduce GHG Emissions", Journal of Lightwave Technology, Vol. 27, Dec. 2009, pp. 1941-1946.

 DOI : 10.35291/2454-9150.2022.0170