International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 03 | March - 2022 ISSN: 2582-3930

Cloud-Security Threats and Management

Mrs.Reena Lobo
Assistant Professor
Dept.of Computer Science
AIET, Mijar

Ashish Menezes
B.E
Dept.of Computer Science
AIET, Mijar

B A SohanKumar
B.E
Dept.of Computer Science
AIET, Mijar

Jahnavi P C
B.E
Dept.of Computer Science
AIET, Mijar

Karthik H B
B.E
Dept.of Computer Science
AIET, Mijar

Abstract – Cloud computing is a compilation of existing techniques and technologies, packaged within a new infrastructure paradigm that offers improved scalability, elasticity, business agility, faster startup time, reduced management costs, and just-in-time availability of resources.The increasing relevance of information confidentiality in cloud computing has forced companies and information organizations to turn their attention to Information Technology (IT) security certifications and standards. Cloud services are becoming an essential part of many organizations. Cloud providers have to adhere to security and privacy policies to ensure their users' data remains confidential and secure. This paper presents a framework about the potential security threats in cloud and how the threats can be restrained or managed

Keywords – Cloud Computing ,Cloud Security, Visualization, Data Privacy

I. INTRODUCTION

Cloud security (also known as cloud computing security) includes many of the same security controls, technologies, practices and procedures that are used to protect physical data centers, network and compute environments only they are deployed as a service to protect your cloud data.

Cloud security is unique in that the duty of care is shared. Some of the responsibility of securing cloud assets falls to the cloud provider, some to the customer. Most cloud service providers, including Amazon Web Services(AWS), Google Cloud and Microsoft Azure, have some form of a Shared Responsibility Model that outlines who is responsible for their sensitive data and where it lives. According to Amazon, the provider is responsible for "security of the cloud" the infrastructure that runs the cloud services while the customer is responsible for "security in the cloud," or the deployments,

virtual servers and applications that are being run. Cloud operations take some level of visibility and control away from the customer, and as such many believe that cloud security is more difficult to achieve than traditional data security. That is partially true, but cloud security may in some ways be easier to manage than on-premise security. The cloud provider bears some of the load for securing operations, and moreover the cloud security systems offer users the ability to manage cloud assets from a central location or dashboard. In addition, the cloud also reduces some of the strain of physical security and network-level security for the customer. In short, cloud security doesn't have to be overwhelmingly difficult if implemented correctly Cloud Computing Industry is growing. According to Gartner, worldwide cloud services revenue is on pace to surpass **$56.3 billion** in 2009, a **21.3% increase** from 2008 revenue of $46.4 billion, according to Gartner, Inc. The market is expected to reach **$150.1 billion in 2013**. Businesses are increasing Cloud adoption We expect a great deal of migration towards cloud computing within the federal government in addition to the already robust private sector growth. The growth of the cloud should not outpace our ability to protect the data that goes into it.

II.CLOUD SECURITY OVERVIEW

Secure cloud computing encompasses three core capabilities: confidentiality, integrity, and availability. Confidentiality is the ability to keep information secret from people who shouldn't have access. Integrity means that systems operate as they are intended to function and produce outputs that are not unexpected or misleading. Availability speaks to maintaining service uptime for cloud infrastructure and cloud-based services, which includes preventing denial-of-service (DoS) attacks. Security is only as strong as the layer below it. Businesses that are crafting their cloud security policies need to consider a "defense in depth" strategy. This means building from the ground up with a trusted foundation in the hardware layer. Applications and software in the cloud will run more securely when they are deployed on a secure foundation.

Why is cloud security important?

For businesses making the transition to the cloud, robust cloud security is imperative. Security threats are constantly evolving and becoming more sophisticated, and cloud computing is no less at risk than an on-premise environment. For this reason, it is essential to work with a cloud provider that offers best-in-class security that has been customized for your infrastructure.Cloud security offers many benefits, including:

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.

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 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.

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.

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.

More and more organizations are realizing the many business benefits of moving their systems to the cloud. Cloud computing allows organizations to operate at scale, reduce technology costs and use agile systems that give them the competitive edge. However, it is essential that organizations have complete confidence in their cloud computing security and that all data, systems and applications are protected from data theft, leakage, corruption and deletion .All cloud models are susceptible to threats. IT departments are naturally cautious about moving mission-critical systems to the cloud and it is essential the right security provisions are in place, whether you are running a native cloud, hybrid or on-premise environment. Cloud security offers all the functionality of traditional IT security, and allows businesses to harness the many advantages of cloud computing while remaining secure and also ensure that data privacy and compliance requirements are met.

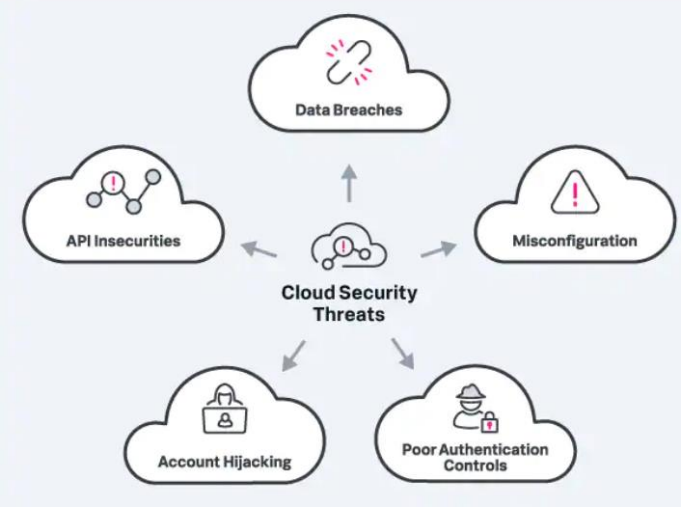
Fig 1-Cloud Security Overview

This concentrates on system vulnerabilities which are a consequence of this core biometric challenge. Since biometric systems are implemented on server computers, they are vulnerable to all cryptographic, virus and other attacks which plague modern computer systems. A practical biometric system should meet the specified recognition accuracy, speed, and resource requirements, be harmless to the users, be accepted by the intended population, be easy to use and be sufficiently robust to various fraudulent methods and attacks on the system. Biometrics are believed to provide solutions to a wide range of problems involving identity checking in the context of national ID programmers' in developing countries.

III.SECURITY THREATS AND MANAGEMENT

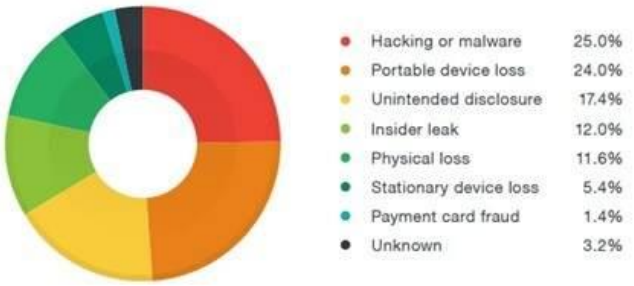
Cloud users are a prime target for malevolent hackers, and protecting complex cloud environments is no small feat for organizations. Experts at the Cloud Security Alliance have identified the following 11 critical threats to cloud computing (ranked in order of severity), referred to as the "Egregious Eleven:"

i. Data breaches. Security responsibility: customer and cloud-service provider
ii. Misconfiguration and inadequate change control. Security responsibility: customer
iii. Lack of cloud security architecture and strategy. Security responsibility: customer
iv. . Insufficient identity, credential, access and key management. Security responsibility: customer
v. Account hijacking. Security responsibility: customer and cloud-service provider
vi. Insider threat. Security responsibility: customer
Insecure interfaces and APIs. Security responsibility: customer and cloud-service provider.



A. DATA BREACHES

A **data breach** is an incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner. A small company or large organization may suffer a data breach. Stolen data may involve sensitive, proprietary, or confidential information such as credit card numbers, customer data, trade secrets, or matters of national security.The effects brought on by a data breach can come in the form of damage to the target company's reputation due to a perceived 'betrayal of trust.' Victims and their customers may also suffer financial losses should related records be part of the information stolen. Based on the number of data breach incidents recorded between January 2005 and April 2015, personally identifiable information (PII) was the most stolen record type while financial data came in second.



Breach methods observed across industries

Most data breaches are attributed to hacking or malware attacks. Other frequently observed breach methods include the following:

- **Insider leak:** A trusted individual or person of authority with access privileges steals data.
- **Payment card fraud:** Payment card data is stolen using physical skimming devices.
- **Loss or theft:** Portable drives, laptops, office computers, files, and other physical properties are lost or stolen.
- **Unintended disclosure:** Through mistakes or negligence, sensitive data is exposed.
- **Unknown:** In a small of number of cases, the actual breach method is unknown or undisclosed

Phases of a Data Breach

- **Research**

The attacker, having picked a target, looks for weaknesses to exploit: employees, systems, or the network. This entails long hours of research on the attacker's part and may involve stalking employees' social media profiles to find what sort of infrastructure the company has.

- **Attack**

Having scoped a target's weaknesses, the attacker makes initial contact either through a network-based or social attack. In a **network-based** attack, the attacker exploits weaknesses in the target's infrastructure to instigate a breach. These weaknesses may include, but are not limited to SQL injection, vulnerability exploitation, and/or session hijacking. In a **social** attack, the attacker uses social engineering tactics to infiltrate the target network. This may involve a maliciously crafted email sent to an employee, tailor-made to catch that specific employee's attention. The email can phish for information, fooling the reader into supplying personal data to the sender, or come with a malware attachment set to execute when downloaded.

- **Exfiltrate**

Once inside the network, the attacker is free to extract data from the company's network. This data may be used for either blackmail or cyberpropaganda. The information an attacker collects can also be used to execute more damaging attacks on the target's infrastructure.

B. API INSECURITIES

Attackers over the past three years have begun to actively target the digital keys used to secure the Internet infrastructure. Stuxnet's creators stole code-signing keys and then used them to allow the malware to more easily evade host-based security. An alleged Iranian hacker broke into a partner of registry Comodo and bought Secure Sockets Layer (SSL) keys for major domains to eavesdrop on activists. And unknown attackers stole important information on RSA's SecureID token, a device that generates one-time keys to strengthen online security. The unique codes that applications in the cloud use to identify one another could be next, security experts say. So-called API keys are used by Web and cloud services to identify third-party applications using the services. If service providers are not careful, an attacker with access to the key can cause a denial-of-service or rack up fees on behalf of the victim.

"It was created as a fairly nonauthoritative identifier -- it was only there to identify applications or the application's use of an API," says K. Scott Morrison, chief technology officer of Layer7 Technologies, a provider of Web security and governance products. "The problem is that developers have started using API keys for stuff that matters." The problem is not any inherent weakness in the keys, but that developers use them for security

when they ought not, he says. In many implementations, the keys are used to identify users, even though the technology was not meant as a way to authorize access to data. And after expanding the power of the keys, developers do not treat them as critical assets. Instead, companies fail to keep track of the keys, e-mailing them around and storing them on desktop hard drives.

C. MISCONFIGURATION

Cloud misconfiguration refers to any glitches, gaps, or errors that could expose your environment to risk during cloud adoption. These cyber threats come in the form of security breaches, external hackers, ransomware, malware, or insider threats that use vulnerabilities to access your network.

The NSA considers cloud misconfiguration a leading vulnerability in a cloud environment. While these risks are often less sophisticated, the issues' prevalence is generally through the roof.

Misconfiguration is a cloud computing problem because multi-cloud environments can be quite complicated, and it can be tough to detect and manually remediate mistakes. According to a Gartner survey, these issues cause 80% of all data security breaches, and until 2025, up to 99% of cloud environment failures will be attributed to human errors.

This is tricky, considering there's no one-time remedy for cloud misconfiguration issues like cloud leaks. However, it would help to implement security procedures at the build stage. So, DevOps and security teams must work collaboratively.

Common Cloud Misconfigurations and Their Solutions

Let's take a deep dive into the most common cloud misconfigurations that you'll likely have to deal with when migrating to a cloud environment.

1. Unrestricted Inbound Ports

All ports open to the internet can be potentially problematic. Cloud services mostly use high-number UDP or TCP ports to prevent exposure risks, but determined hackers can still sniff them out. Obfuscation can be helpful, but it's insufficient by itself When migrating to a multi-cloud environment, make sure you know the full range of open ports and then restrict or lock down those that aren't strictly necessary.

2. Unrestricted Outbound Ports

These ports create opportunities for security events like data exfiltration, lateral movement, and internal network scans once there's a system compromise. Granting outbound access to RDP or SSH is a common cloud misconfiguration. Application servers seldom have to SSH to other network servers, so it's unnecessary to use open outbound ports for SSH.

Make sure you limit the outbound port access and use the least privilege principle to restrict outbound communications.

3. Secrets Management

This configuration issue can be damaging to your organization. Securing secrets like API keys, passwords, encryption keys, and admin credentials is essential. But most companies openly avail these through compromised servers, poorly configured cloud buckets, HTML code, and GitHub repositories. This is as risky as leaving your home's deadbolt key taped to your front door.

You can beat this by maintaining an inventory of all your company secrets in the cloud and regularly evaluating how they're secured. Otherwise, threat actors could easily breach your systems, access your data, and overrun your cloud resources to effect irreversible damage.

You may also use secret management solutions and services like Hashicorp Vault, AWS Secrets Manager, Azure Key Vault, and AWS Parameter Store.

4. Disabled Monitoring and Logging

Surprisingly, most organizations fail to configure, enable, or review the telemetry data and logs offered by public clouds, which can be sophisticated. It would help to have someone responsible for regular reviews and flagging security-related incidents.

This valuable tip isn't only limited to IaaS public clouds. You'll also get the same information from storage-as-a-service vendors, which you must also review regularly. A maintenance alert or update bulletin could leave your organization with profound security implications, but it won't help if there's no one paying attention.

5. ICMP Left Open

The ICMP (Internet Control Message Protocol) reports network device errors, but it's a common target for threat actors. This happens because while the protocol can display if your server is responsive and online, cybercriminals can also use it to pinpoint an attack.

Furthermore, it's also an attack vector for denial-of-service (DDoS) and many types of malware. A ping flood or ping sweep can overwhelm your servers with ICMP messages. While it's a dated attack strategy, it's still effective. So make sure your cloud configuration blocks ICMP.

6. Insecure Automated Backups

Insider threats to your cloud environment are an ever-present cybersecurity risk. According to McAfee, about 92% of business organizations have workers' credentials being sold on the darknet. One section where insider threats can be particularly damaging is when you fail to secure automated cloud data backup properly.

You may have protected your master data, but poorly configured backups will inadvertently remain vulnerable and exposed to insider threats.

When migrating to the cloud, ensure your backups are encrypted whether at rest or in transit. Also, verify the permissions to restrict access to the backups.

7. Storage Access

Most cloud users believe that "authenticated users" only cover those already authenticated within the relevant apps or organizations regarding storage buckets. Unfortunately, this isn't the case.

"Authenticated users" refers to any person with AWS authentication, essentially any AWS client. Due to this misunderstanding, alongside the resulting control settings misconfiguration, you may have your storage objects wholly exposed to public access. Be especially cautious when setting storage object access to grant it to only the people within your organization.

IV. MANAGEMENT TECHNIQUES

1.CONFIDENTIALITY

Data must be encrypted before it is outsourced, to protect it from malicious internal or external attacks. Data confidentiality is the process of protecting data from illegal access and disclosure from the outsourced server and unauthorized users. This is done by encrypting the data so that only the authorized users can decrypt it.

2. INTEGRATED SECURITY BETWEEN CLOUDS

Whenever any customer demands resources from different cloud platforms due to various reasons, there arises the need of much more security between the cloud and the customer. To work as a single entity for a particular customer, there is a need for security that works in an integrated manner so that operability becomes simple for any user keeping the applications secure.

V. CONCLUSION

Cloud computing is recently new technological development that has the potential to have a great impact on the world. It has many benefits that it provides to it users and businesses. For example, some of the benefits that it provides to businesses, is that it reduces operating cost by spending less on maintenance and software upgrades and focus more on the businesses it self. But there are other challenges the cloud computing must overcome. People are very skeptical about whether their data is secure and private. There are no standards or regulations worldwide provided data through cloud computing. Europe has data protection laws but the US, being one of the most technological advance nation, does not have any data protection laws. Users also worry about who can disclose their data and have ownership of their data. But once, there are standards and regulation worldwide, cloud computing will revolutionize the future.. Cloud computing provides advanced computing resources available on-demand, that scale as needed, with regular updates and without the need to buy and maintain an on-premise infrastructure. With cloud computing, teams become more efficient and reduce time to market as they can rapidly acquire, scale services, without the considerable effort that requires managing a traditional on-premise infrastructure

VI. REFERENCES

1. Cloud Security Alliance ,2013, The Notorious Nine: Cloud Computing Top Threats in 2013, p8-p21.
2. NIST, NIST Cloud Computing Reference Architecture, 2011 Privacy and data protection,Vol 7 Issue 4, IT compliance and IT security-Part 1, Dr. Jörg Hladjk, p 3-4
3. William R. Cheswick and Steven M. Bellovin. Firewalls and Internet Security: Repelling the Wily Hacker. Addison-Wesley, Reading, MA, 1st edition, 1994.
4. Boroojeni, Kianoosh G., M. Hadi Amini, and S. S. Iyengar. "Cloud Network Data Security." Smart Grids: Security and Privacy Issues. Springer, Cham, 2017. 71-82.
5. Chang, Jeffrey, and Mark Johnston. "Approaches to Cloud Computing in the Public Sector: Case Studies in UK Local Government." Advanced Research on Cloud Computing Design and Applications. IGI Global, 2015. 51-72.
6. Perception Point. Analysis and Exploitation of a Linux Kernel Vulnerability (CVE-2016-0728). Accessed June 8, 2016. http://perception-point.io/2016/01/14/analysis-and-exploitation-of-alinux-kernel-vulnerability-cve-2016-0728/

.