Security Threats and Countermeasures In Cloud Computing

Falalu Abdulrauf Musa
Department of Computer Science
Federal Polytechnic Kaura-Namoda
Zamfara State, Nigeria.
Abdulfmusa@yahoo.com

Shamsudeen Muhammad Sani
Department of Computer Science
Federal Polytechnic Kaura-Namoda
Zamfara State, Nigeria.
Shamsusani78@yahoo.com

***Abstract* - Security issues have given rise to immerse an active area of research because of the many security threats that many organizations have faced today. Addressing these issues requires gaining the trust of application users and cloud services. In this research paper, we highlighted the major threats to the security of cloud systems, while introducing the most appropriate responses. We mentioned and discussed the latest potential threats. After some effective countermeasures are listed and explained.**

***Keywords*: security challenges, cloud computing, threat and countermeasures**

I. INTRODUCTION

Cloud computing is a new concept that was brought into the business environment, where users can interact directly with virtual resources and save costs for consumers. There are several models for implementing cloud computing services which help in retrieving information. The three cloud computing models: Software as a Service (SaaS), platform as a service (PaaS) and Infrastructure as a Service (IaaS). There are several models for data protection in the cloud. Security in the cloud is made up of the security features of browser and Web services framework. This paper describes in detail the security risks in cloud computing; types of threats and solutions to these threats (Hashizume, 2013).

II. WHAT IS CLOUD COMPUTING?

The term cloud computing refers to applications and services offered over the Internet. Data centers all over the world offer these services, which collectively are referred to as "cloud". The name cloud computing was inspired by the cloud symbol that is often used to represent the Internet in flowcharts and diagrams (Lalbeg & S. Mulik, 2011).

The idea of ”cloud” simplifies the number of network connections and computer systems involved in online services. Anyone with an Internet connection can access the cloud and the services it offered. Because these services are often connected, users can share information on multiple systems and with other users (Patidar, 2016).

A. Models of Cloud Computing

Cloud services are divided into three categories: Software as a Service (SaaS), Platform as a Service (PaaS) and infrastructure as a service (IaaS). SaaS services are provided by service providers and customers to use these services to run applications on a cloud infrastructure. These applications can be accessed via the browser. PaaS is a form of renting hardware, operating systems, storage and networking capacity on the Internet. The service delivery model allows customers to rent virtualized servers and associated services for running existing applications or developing and testing new applications. In IaaS consumer is provided with power to process control, storage management, networking and other basic computer resources which are useful for the management of any software (Zhang, Cheng &Boutaba, 2010;Expert Group Report, 2010).

III. SECURITY

When multiple organizations share resources there is a risk of data misuse. So, to avoid the risk, it is necessary to secure data repositories and also the data that involves storage, transit or process. Data protection is the most important challenge in the cloud computing. To improve security in the cloud, it is important to provide authentication, authorization, and access control to the data stored in the cloud (Kapoor, 2013). The three main areas in the data security are:

A. Confidentiality

Confidentiality is typically provided through customer data encryption. Data may be at the volume storage level or object-level storage. Volume storage encryption prevents snapshot, cloning or exposure, exploration by the cloud provider, and exposure because of the loss of the physical drives. IaaS volumes can be encrypted using instance-manage encryption (instance managed, keys stored in the volume and protected by a secret or key pair), externally managed encryption (instance managed, the keys are managed externally, provided on request)

IRJECE

or proxy encryption (external software or managed device). Object or file encryption allows the user to deploy virtual private storage (VPS). Like a virtual private network, VPS allows the use of a public shared infrastructure while still protecting data, since only those with the encryption keys can read the data. The objects can be encrypted by standard tools, or with the applications using the data, or by a proxy before being placed in storage. IaaS providers may also offer IAM policies and access control lists (ACLs) to further protect stored data. The transfer of data is also protected by provider-implemented SSL VPN connections (Kanday, 2012;Expert Group Report, 2010)

B. Integrity

In addition to data confidentiality, the customer must also consider the integrity of their data. Confidentiality does not mean integrity. Data can be encrypted for confidentiality reasons, but the customer might not have a method to validate the integrity of that data. IaaS providers should regularly check for integrity by keeping track of data checksums and repair data if corruptions are detected by using redundant data. The data in the transfer must also be checksum validated to detect corruption (Rajeev, 2012)

C. Availability

Suppose customer data maintained its confidentiality and integrity, the customers should also be concerned about the availability of their data. They should be concerned with three main risks: network-based attacks; the cloud service provider's own availability; and backups or redundancy. Availability is usually defined in SLAs and customers pay for different levels of availability based on their risk tolerances. IaaS providers can provide redundant storage (geographic and systemic), versioning and high bandwidth connectivity to avoid problems arising from availability issues (Kapoor, 2013)

IV. DATA SECURITY CHALLENGES

As we are moving to cloud model based on the Internet, it requires a strong emphasis on data security and privacy. Loss of data or data leakages could have severe impact on business, brand, and trust of an organization.

A. Threat: Data Breaches

A data breach is an event where confidential, protected or sensitive information comes out, seen, stolen or used by a person not authorized to do so. The data breach could be the main focus of a targeted attack or it may simply be a result of human error, software vulnerabilities or poor security practices.

A data breach can result in any kind of information that was not intended for public release, including, but not limited to, personal health information, financial information, personally identifiable information (PII), trade secrets and intellectual property (Cloud Security Alliance, 2011).An organization's cloud-based data can be of value to different parties for different reasons. For example, organized crime often seeks economic, health and personal information to perform a variety of scams. Competitors and foreign nationals may be very interested in trade secrets and intellectual property.Activists can reveal information that could cause harm or embarrassment. Unauthorized insiders acquiring data in the cloud are a major problem for organizations (Y. Rashid, 2016).The risk of data breach is not unique to cloud computing but consistently ranks as the biggest concern for cloud customers. A cloud environment is subject to the same threats as the traditional corporate network, as well as new ways to attack through shared resources, cloud provider personnel of cloud services, their devices, and third-party partners. Cloud services are very affordable and the huge amount of data that they host makes them an attractive target (Fahmida, 2016; Cloud Security Alliance, 2016).

Countermeasure: Cloud providers typically implement security controls to protect the environment, but in the end, organizations have a responsibility to protect their data in the cloud. The best protection against data breach is an effective security program. Two important security measures that can help businesses stay safe in the cloud are multifactor authentication and encryption (). Multifactor authentication (MFA) is a security system that requires more than one method of authentication from independent categories of credentials to verify the identity of users to gain access to the application, or other operations (Sen, 2013).

In Multifactor authentication, two or more independent credentials are combined; password, security token and biometric verification are usually the core requirements. The goal is to create a superimposed protection that will make very difficult for any authorized person to access a target such as a database, network, computing device or physical location. The idea is, if one factor is broken or compromised, the intruder has at least one or more roadblock to breach before successfully getting into the target (Rouse, 2015).

Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Although encryption does not prevent interception, but it denies any unauthorized access to a message content. In an encryption scheme, the content of the communication or message (referred to as plaintext) is encrypted using an encryption algorithm by generating cipher text that can only be read if decrypted. Technically, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, large computational resources and skills are required. An authorized recipient of a message can easily decrypt the message with the key provided by the originator to recipients, but not to unauthorized (SearchSecurity, 2015).

IRJECE

B. Threat: Insufficient Identity, Credential and Access Management

Data breaches and other attacks frequently result from lax authentication, weak passwords, and poor key or certificate management (Info World, 2016). Usually, some organizations struggle with identity management as they try to assign permissions appropriate to the user's job role. Importantly, they sometimes forget to remove user access when a job function changes or when a user leaves the organization (Shah, Shrikanth & Anankade, 2013). According to, Anthem breach has exposed more than 80 million customer records, as a result of stolen user credentials (Rajeev, 2012). Anthem had failed to deploy multifactor authentication, so once the attackers obtained the credentials, it was game over. The system must scale to handle lifecycle management for the huge number of its users. Identity management systems must support immediate de-provisioning of access to resources when personnel changes, such as job termination or role change, occurred (Kapoor, 2010).Organizations planning to unify identity with a cloud provider need to know the security measures the cloud provider uses to protect the identity platform. Centralizing identity into a single repository has its risks. Organizations need to weigh the trade-off of the convenience of centralizing identity against the risk of having that repository become an extremely high-value target for attackers (Cloud Security Alliance, 2016).

Countermeasure: Multifactor authentication systems such as a smartcard, OTP, and phone authentication are required for users and operators of a cloud service because such systems make it harder for attackers to log in with stolen passwords.

This form of authentication helps address password theft, where stolen passwords enable access to resources without user consent. Stealing of password can manifest in common network lateral movement attacks, such as "pass the hash" (Hashizume, Rosado, Eduardo & Fernandez, 2013).

C. Threat: Insecure Interfaces and APIS

Providers of cloud computing exhibit a set of software user interfaces (UIs) or application programming interfaces (APIs) that customers use to manage and interact with cloud services. Provisioning, management, orchestration and monitoring are all performed with these interfaces. The security and availability of general cloud services are dependent on the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy. Organizations and third parties may build on these interfaces to offer value-added services to their customers. Thus, this introduces the complexity of the new layered API; which also increases risk, because organizations may be required to relinquish their credentials to third parties in order to enable their agency (ISACA, 2011).

Therefore, APIs and UIs are generally the most exposed part of a system, perhaps the only asset with an IP address available outside the trusted organizational boundary. These assets will be the target of heavy attack, and adequate controls protecting them from the Internet are the first line of defense and detection (Held, 2016).

Countermeasure: Security-focused code reviews and rigorous penetration testing, so far, are the two reliable countermeasures to this type of attack. Security code review is the process of auditing the source code for an application to verify that the proper security controls are present, and they work as intended and that they have been invoked in all the right places. A penetration test on the other hand, which is also known as pen test, is an attack on a computer system that looks for security weaknesses, potentially gaining access to the computer's features and data. This process typically identifies the target systems and a particular goal then reviews available information and undertakes various means to attain the goal. A penetration test target may be a white box (which provides background and system information) or black box (which provides only basic or no information except the company name). A penetration test can help determine whether a system is vulnerable to attack if the defenses were sufficient and which defenses (if any) the test defeated (Penetration Guidance Interest Special Group, 2015).

D. Threat: System Vulnerabilities

System vulnerabilities are exploitable bugs in programs that attackers can use to infiltrate a computer system for the purpose of stealing data, taking control of the system or disrupting service operations. Using vulnerabilities within the components of the operating system like the system kernel, libraries, and application tools; to put the security of all services and data at significant risk (Fahmida, 2016). Although this type of threat is common; bugs have been a problem since the invention of computers; they became exploitable remotely when networks were created. The introduction of multi-tenancy in cloud computing that allows systems from various organizations to be placed to each other in close proximity, and give them access to shared memory and resources, creates a new attack surface (Cloud Security Alliance, 2016).

Countermeasure: Attacks on system vulnerabilities can be mitigated with "basic IT processes". Best practices include regular vulnerability scanning, prompt patch management, and a quick follow-up on reported system threats (Cloud Security Alliance, 2016). Vulnerability scanning is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened (Drummond, 2015). A patch, on the other hand, is a piece of software that is designed to update a computer program or its supporting data and to fix or improve it. This includes fixing security

IRJECE

vulnerabilities and other bugs, with such patches usually called bugfixes or bug fixes, and improving the usability or performance (Josh, 2015).

E. Threat: Account Hijacking

Account or service hijacking is not new. Methods of attack such as phishing, fraud and exploitation of software vulnerabilities still yield results. Usually, credentials and passwords are reused, which magnify the impact of such attacks (Fahmida, 2016). Cloud solutions add a new threat to the landscape. If an attacker intrudes into your credentials, they can eavesdrop on your activities and a transaction, which allows them to manipulate your data, return falsified information and redirect your clients to illegitimate sites. Your account or service instances may become a new base for attackers (Cloud Security Alliance, 2016).

Countermeasure: Organizations should be aware of these types of attacks as well as common defense-in-depth protection strategies to contain the damage – and possible litigation – resulting from a breach. They should look to prohibit the sharing of account credentials among users and services and leverage strong two-factor authentication techniques where possible. All accounts and account activities should be monitored and traceable to a human owner, even service accounts. The key is to protect account credentials from being stolen (Cloud Security Alliance, 2016).

F. Threat: Malicious Insiders

CERN says "an insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's data or network, system, and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems." It's easy to misconstrue a bungling attempt to perform a routine job as "malicious" insider activity.

For example, an administrator can accidentally copy a sensitive customer database to a publicly accessible server (Trzeciak, 2011).

Countermeasure: It's recommended that organizations should control the encryption process and keys, segregating duties and minimizing access given to users. Effective logging, monitoring, and auditing administrator activities are also critical (Y. Rashid, 2016).

G. Threat: Advanced Persistent Threats

Advanced Persistent Threats (APTs) are a parasitical form of cyber-attack that penetrates systems to establish a foothold in the computing infrastructure of target companies from which they smuggle data and intellectual property. APTs pursue their goals stealthily over extended periods of time, often adapting to the security measures intended to defend against them. Spear phishing, direct hacking systems, delivering attack code through USB devices, penetration through partner networks and use of unsecured or third-party networks are common points of entry for APTs. Once in place, APTs can move laterally through data center networks and blend in with normal network traffic to achieve their objectives (Cloud Security Alliance, 2016). APTs typically move laterally through the network and blend in with normal network traffic, making it very difficult to be detected.

Major cloud providers apply advanced techniques to prevent APTs from penetrating their infrastructure. Common points of entry include spear phishing; direct attacks, USB drives preloaded with malware, and compromised third-party networks (Y. Rashid, 2016).

Countermeasure: Organizations' IT departments should be sensitized about the latest advanced cyber security attacks that target companies and government organizations. Although APTs can be difficult to detect and eliminate, some can be stopped with proactive security measures. For example, it is critical that users be educated to recognize and handle social engineering techniques such as spear phishing that are commonly used to introduce APTs (). Awareness programs that are regularly reinforced are one of the best defenses against these types of attacks because many of these vulnerabilities require user intervention or action. Staff should be well-established and think twice before opening an attachment or clicking a link (Zaharia, 2016).

H. Threat: Permanent Data Loss

For both consumers and businesses, the prospect of permanently losing one's data is terrifying. As the cloud has developed, reports of permanent data loss due to provider error have become extremely rare. But malicious attackers have been known to permanently delete cloud data to harm businesses, and cloud data centers are as vulnerable to natural disasters as any facility (Data Security Alliance, 2016).

Countermeasure: Cloud service providers cannot prevent data loss. Customers need to encrypt data before uploading it to the cloud, and then the customers must be careful to protect the encryption key. Once the key is lost, so is the data. Moreover, some cloud providers recommend distributing data and applications across multiple zones for added protection. Adequate data backup measures are essential, as well as adhering to best practices in business continuity and disaster recovery. Daily data backup and off-site storage remain important within the cloud environments (Nate, 2016).

I. Insufficient Due Diligence

Organizations that adopt the cloud without fully understanding the environment and its associated risks may encounter a "myriad of commercial, financial, technical, legal,

IRJECE

and compliance risks," (Cloud Security Alliance, 2016). Due diligence applies whether the organization is trying to migrate to the cloud or merging (or working) with another company in the cloud. For example, organizations that fail to scrutinize a contract may not be aware of the provider's liability in case of data loss or breach. Some organizations have operational and architectural problems especially if their teams are not familiar with cloud technologies their applications may be deployed to a particular cloud. According to Jason Weinstein, who summarized the issue of cyber security due diligence succinctly when he said: "When you buy a company, you're buying their data, and you could be buying their data-security problems"(Y.Rashid, 2016).

Countermeasure: Organizations moving to a cloud technology model must perform extensive due diligence to understand the risks they assume by adopting this technology model and engaging the suppliers who provide it (ISACA, 2011).

J. *Threat: Denial Of Service (DoS)*

Denial-of-service (DoS) attacks have been around for years; they are attacks meant to deny users of a service from being able to access their data or their applications. When an attacker launches a DoS attack, the targeted cloud service consumes inordinate amounts of finite system resources such as processor power, memory, disk space or network bandwidth. Similarly, in distributed denial-of-service (DDoS) attacks which cause an intolerable system slowdown and leaves all legitimate service users confused and angry as to why the service is not responding. DoS attacks consume large amounts of processing power, a bill the customer may ultimately have to pay. On the other hand, DDoS attacks are also common, and organizations should be aware of asymmetric, application-level DoS attacks, which target Web server and database vulnerabilities (Wikipedia, 2016).

Countermeasure: It's not possible to fully prevent Denial of Service attack from affecting an organization's network, but there are steps that if taken can prevent them. However, these are some things you can do to reduce the risk of Denial of Service attacks:

- Purchasing a lot of bandwidths. Although it's expensive, but tons of bandwidth makes perpetrating a DoS attack much more difficult because it's more bandwidth that an attacker has to clog (Rubens, 2013).
- Using DoS attack detection technology. Intrusion prevention system and firewall manufacturers now offer DoSprotection technologies that include signature detection and connection verification techniques to limit the success of DoS attacks (Meyran, 2012).
- Preparing for DoS response. The use of throttling and rate-limiting technologies can reduce the effects of a DoSattack. One such response mode stops all new inbound connections in the event of a DoS attack, allowing established connections and new outbound connections to continue (Rubens, 2013).

V. CONCLUSION

Cloud computing is a new term that is introduced in a business environment where users can interact directly with the virtualized resources and save the cost for the consumers.Some security issues and their countermeasures are discussed in this research paper. Some crucial and well-known security attacks along with their possible solutions are studied too. Security in the cloud needs to be constantly updated to ensure that they are not riddled by attacks. The domain of security in the cloud will be the deciding factor in the success or failure of a cloud system in the future.

REFERENCES

[1] Rajeev Kanday, "A Survey on Cloud Computing Security," 2012 International Conference on Computing Sciences, October, 2012

[2] Priya Kapoor, "Security Attacks and Countermeasures," International Journal of Science, Engineering &Computer Technology, January, 2013

[3] Tim Mather, Subra Kumaraswamy&Shahed Latif, Cloud Security & Privacy: An Enterprise Perspective on Risks & Compliance, CA: O'Reilly Media, Inc., 2009

[4] Expert Group Report, The Future of Cloud Computing: Opportunities For European Cloud Beyond 2010, European Commission Information Society and Media, 2011

[5] Cloud Security Alliance, The Treacherous 12: Top Threats Working Group, Cloud Computing Top Threats in 2016

[6] Qi Zhang, Lu Cheng &RaoufBoutaba, "Cloud computing: state-of-the-art and research challenges," The Brazilian Computer Society, April, 2010

[7] Harit Shah, Sharma Shankar &AnandaneShrikanth, "Security Issues on Cloud Computing," International Journal of Computer Science and Information Security, Vol. 11, No. 8, August 2013

[8] ISACA, IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud: US National Institute of Standards and Technology (NIST) Special Publication, USA, 2011

[9] Margaret Rouse (2008). *HIDS/NIDS (host intrusion detection systems and network intrusion detection systems).* Retrieved October 25th, 2016 from http://searchsecurity.techtarget.com/definition/HIDS-NIDS

[10] Paul Rubens (2013). *6 Tips for Fighting DDoS Attacks.* Retrieved October 26th, 2016 from http://www.esecurityplanet.com/network-security/5-tips-for-fighting-ddos-attacks.html

[11] Wikipedia (2016). Denial-of-service attack. Retrieved October 26th, 2016 from https://en.wikipedia.org/wiki/Denial-of-service_attack

[12] Nate Lord (2016). *27 Data Security Experts Reveal The #1 Information Security Issue Most Companies Face with Cloud Computing & Storage.* Retrieved October 27th, 2016 from

IRJECE

https://digitalguardian.com/blog/27-data-security-experts-reveal-1-information-security-issue-most-companies-face-cloud

[13] Fahimda Y. Rashid (2016). *The dirty dozen: 12 cloud security threats.* Retrieved September 26th, 2016 from http://www.infoworld.com/article/3041078/security/the-dirty-dozen-12-cloud-security-threats.html

[14] Randy Trzeciak (2011). *Network Security, Incident Management, and Insider Threats in the Healthcare Industry.* Retrieved September 28th, 2016 from http://csrc.nist.gov/news_events/HIPAA-May2011_workshop/presentations/day2_HIPAA-conference2011-Insider-Threat.pdf

[15] Josh Drummond (2015). *What is vulnerability scanning?*Retrieved September 29th, 2016 from http://www.oit.uci.edu/security-tips/what-is-vulnerability-scanning/

[16] Keiko Hashizume, David G. Rosado, Eduardo Fernandez-Medina & Eduardo B. Fernandez (2013). *An analysis of security issues for cloud computing.* Retrieved September 30th, 2016 from https://jisajournal.springeropen.com/articles/10.1186/1869-0238-4-5

[17] Cloud Standards Customer Council (2015). *Practical Guide to Platform as-a-service.*Retrieved August 24th, 2016 from http://www.cloud-council.org/CSCC-Practical-Guide-to-PaaS.pdf

[18] Security Standards Council, Information Supplement: Penetration Testing Guidance Penetration Test Guidance Special Interest Group: PCI Security Standard Council, 2015

IRJECE