Cloud Computing Security: Latest Issues & Countermeasures

Shelveen Pandey, Mohammed Farik

Abstract: Cloud computing describes effective computing services provided by a third-party organization known as cloud service provider for organizations to perform different tasks over the internet for a fee. Cloud service provider's computing resources are dynamically reallocated per demand, and their infrastructure, platform, and software, and other resources are shared by multiple corporate and private clients. With the steady increase in the number of cloud computing subscribers of these shared resources over the years, security on the cloud is a growing concern. In this review paper, the current cloud security issues and practices are described and a few innovative solutions are proposed that can help improve cloud computing security in the future.

Index Terms: Cloud Computing, Security Countermeasures, Security Threats

1 Introduction

CLOUD computing (also known as "the cloud") provides client users with significant cost savings, both in terms of capital and operational expenses. It also allows them to implement cutting-edge technologies to meet their information processing needs and adopt pay-per-use model. The three common cloud services are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). One of the main areas that is of major concern is the security aspect of cloud computing. Both, the cloud providers as well as the clients need to be fully aware of the security threats and apply better countermeasures to protect resources. The cloud services providers (CSVs) need to protect their infrastructure, platform, and software from attacks, while the clients of the cloud need to protect their data, when using cloud services.

2 Service Model

Fig. 1 shows the diagram representing cloud service model with a few service providers mentioned for each type of service. *Software as a Service* (SaaS) allows clients to run online applications. These consumers use the Providers CSV's application running on a cloud infrastructure. The cloud user does not manage the cloud infrastructure such as network, server's storage and operating systems. SaaS is the easiest way to cloud compute where off-the-shelf applications are accessed over the internet. *Platform as a Service* (PaaS) allows users to create their own applications using supplier specific tools and languages at a very low cost. Also, network and operating systems are not administered by the consumer. *Infrastructure as a Service* (IaaS) allows users to run any application they please on cloud hardware of their own choice where existing applications can be migrated from a company datacenter in order to reduce its costs.

- *Shelveen Pandey is currently pursuing Postgraduate Diploma in Information Technology in the School of Science and Technology at The University of Fiji.*
- *Mohammed Farik is a Lecturer in Information Technology in the School of Science and Technology at The University of Fiji.*
- *Email: mohammedf@unifiji.ac.fj*

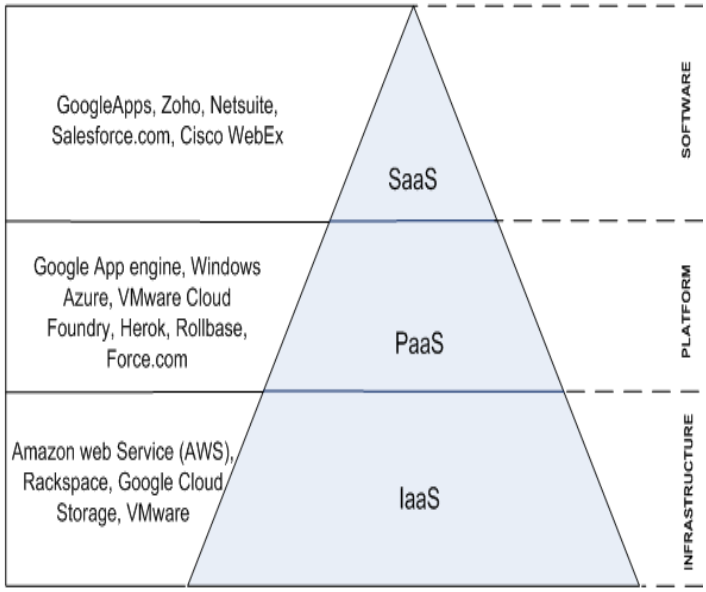

Fig. 1 *Cloud Computing Services*

3 Security Issues and Countermeasures

The top cloud computing threats include data breaches, data loss, account hijacking, insecure API's, denial-of-service, malicious insiders, abuse of service, insufficient due-diligence, and shared technology. In this section, these threats are described with countermeasures.

3.1 Data Breaches

In cloud computing, the *virtual machines* (VMs) are residing in the same physical host and when one VM is able to access information from another VM, data breach occurs. The major risk factor is when the tenants of the two VMs are different customers. Data can be breached from highly sophisticated secured servers to poorly designed multi-tenant database where a flaw in the client's application can lead the hacker to access client's information and also information of every other client. Also, the rise of *Web 2.0* applications and SaaS has increased the chances of side-channel attacks (nonintrusive attacks) even though transmission between web browser and server are encrypted through HTTPS and Wi-Fi encryption). Some of side-channel attacks [1] are described in Table 1, with some countermeasures [2], [3] in Table 2.

TABLE 1
SIDE-CHANNEL ATTACKS

Side-Channel Attack Types	Description
Timing Attacks	Are attacks based on measured time that various cryptographic algorithms take to complete execution
Power-monitoring attack	Make use of varying power consumption of the hardware during computation
Electromagnetic attacks	Are based on leaked electromagnetic radiation, which can directly provide plaintexts and other information.
Acoustic cryptanalysis	Are attacks that exploit sound produced during a computation
Differential fault analysis	Discovers secrets by introducing faults in a computation
Data remanence	Sensitive data are read after supposedly having been deleted
Row hammer - off	More RAM/CPU bandwidth is spent on refresh than actual task

TABLE 2
DATA BREACH COUNTERMEASURES

Countermeasures	Description
Encryption	Encrypt all files, devices, and systems when storing, sending, or receiving using the best standards. Maintain strict enforcement of encryption policy.
Fragmentation-redundancy-scattering (FRS)	A technique that provides intrusion tolerance by breaking down sensitive data into insignificant fragments and transported in redundant ways across different sites of the distributed system.
Digital signature	Secures the data with RSA algorithm while data is being transferred across the internet
Homographic encryption	Is used to secure data in cloud by performing arbitrary computation on cipher-texts without it being decrypted, but may consume extra CPU, power, and affect response time.
Bring your own device (BYOD)	BYOD devices may be infected with malware, spyware or virus that can infect a company's Intranet and PCs. A solution is to provide your employees with the necessary working tools.
Strong Password	Enforce the use passwords that have at least an ideal length of 12 characters, composed of cardinality 94, and have at least 78.6 bits entropy. Ensure that all the devices such as Computers, Tablets and smart phones are password protected.

3.2 Data Loss

There are a lot of ways data can be lost in cloud. Some of the reasons that could lead to permanent loss of data include malicious attacker, hard drive failure, fire or earthquake. Some of these reasons could be due to the service providers fault. Also, if the user encrypts the data and loses the encryption key, data cannot be recovered. Data protection should be done at different levels such as *data in transit*, *data at rest* and *data in use*. There are many *data loss prevention* (DLP) tools that can be chosen by organizations as per need. While *data backup* and *encryption* are the key countermeasures, there are some other new ways. *Geo-redundant storage* by *Azure* supports high availability for applications like scaling to multiple instances amongst others. *GRS* provides protection against major datacenter failures which asynchronously replicates six copies of the data across different sites of which three copies are sites on the same site and the other three are located at a different geographic region [4]. Others such as network encryption, access controls, intrusion detection, prevention and Security training should also be implemented. Also, organizations should not link accounts together where one account is daisy chained to other accounts where there are highly chances if one account is hacked, the hackers gain access to all the other accounts it is linked to. Furthermore, service agreements containing privacy and security should be reviewed to update the terms and policies and the customers notified on a regular basis.

3.3 Account Hijacking

TABLE 3
ACCOUNT HIJACKING COUNTERMEASURES

Countermeasures	Description
Two-factor Authentication	To gain access to the cloud account only a password is required and a better solution is to have two-factor authentication (is a security process in which the user provides two means of identification for separate categories e.g. one is a card and the other is a security code) . Organizations should also prohibit sharing of accounts credentials between users and services.
Identity and Access Management Guidance	Includes centralized directory, access management, identity management, role-based access control, user access certifications, privileged user and access management, separation of duties and identity and access reporting.
Dynamic credentials	Uses an algorithm to create dynamic credentials for mobile cloud computing systems. The dynamic credentials change its value once a user changes its location or when he has exchanged a certain number of data packets. *Wallix-adminbastion on Demand* (WOD) is a privileged access management solution for the cloud where this solution delivers management, control and auditing of privileged user access in cloud.

Account hijacking or *service hijacking* uses attack methods such as phishing, fraud and exploitation of software vulnerabilities where credentials and passwords are reused. If an attacker gains access, they can eavesdrop on your transactions, manipulate the data and make the data untrustworthy. If the attacker gains access to the cloud VM that hosts our website, they can run malicious code and re-direct clients to illegitimate sites or make it inaccessible. Table 3 describes some countermeasures to prevent account hijacking [2].

3.4 Insecure API's

We have seen that the users communicate through API's and they are accessible from anywhere over the internet. Malicious attackers can use them and compromise confidentiality, availability, accountability and integrity. Cloud API's are basically software interfaces, typically standard-based which the cloud providers make available for the customers in managing their cloud services. Some of the important issues the users should be focusing on are the transport security, authentication and authorization, code and development practices and message protection [5], [6]. Table 4 provides some countermeasures against insecure APIs.

TABLE 4
INSECURE API'S COUNTERMEASURES

Countermeasures	Description
Documentation	The users can ask for documentation of their API's and any existing assessment results /reports that shows security best practices and audit results.
OAUTH (Open Authorization)	OAUTH is a significant step forward but if it will not solve problems if people do not use it correctly.
Penetration Tests	Customers can be ask by the cloud providers to allow penetration tests and vulnerability assessment to be performed against API's and also the third party provider can perform the tests and the results can be provided back to the customers.
Updates	Any update can change the API settings which can result in application or function to crash so there is a responsibility for the cloud provider to fix the vulnerabilities so that the API bugs can be patched without the end users being affected.
Security Standards	The security standards of the cloud provider should be thoroughly inspected and ensure that strict authentication along with encrypted transmission are populated. By adhering to standards such as SAS-70 (statement on Auditing standards) the vendor will be serious about information security and protecting your data.

3.5 Denial-of-Service

The *Denial-of-service* (DoS) attacks attempts to make the system or network resources unavailable to the users from accessing their data and applications from cloud. This can be temporarily, indefinite interrupt or completely suspend the service of the host. The attacker can disrupt the services in the virtualized cloud environment by using the RAM, CPU, network bandwidth, and disk space. The attacker can also use distributed denial-of-service (DDoS) where more than one unique IP- address are used. Table 5 provides some countermeasures against insecure APIs [7], [8].

TABLE 5
DOS COUNTERMEASURES

Countermeasures	Description
Intrusion Detection Systems (IDS)	A defense mechanism is used for guarding where each cloud is loaded with separate IDS. When a specific cloud is under attack, the cooperative IDS alerts the whole system.
Isolation	One way to preventing DDoS is by isolating non-public applications from the internet and by providing resiliency against cloud outages
Netflow	One solution is to enable Netflow features in router where the traffic can be monitored. Netflow gives a detailed view of the Application flows to the Network Engineers.
Access Control List	Another way is to use Access Control List (ACL) to block offending traffic.

3.6 Malicious Insiders

The employees who are working for cloud service providers such as the system administrator will have complete access to the SaaS, PaaS, and IaaS resources. Their access can be a big threat to customers to view confidential data. Any misuse by malicious insider is possible and hard to detect due to the lack of transparency into providers process and procedure. This affects the core principles of information Security (confidentially, authenticity, authorization, integrity, data protection, accountability and non-repudiation) [9]. Countermeasures include implementing a tracking system which can generate reports of employee's activities. Also, a client- side encryption gateway can ensure that access to the encryption key is controlled only by the enterprise, and not by the cloud service provider or a third-party encryption provider [10]. So, even if the data is intercepted, the hackers will not be able to view the clear data since it will remain encrypted and safe. Client side encryption is a way to protect data since the encryption is done locally within the client's browser and the private key is never transmitted to the server which leaves the data protected.

3.7 Abuse of Cloud Service

The main concern is for the CSVs rather than cloud service clients since the users will be trying to hack the system to gain access to confidential data. Anyone with a card can sign up for a free limited time period which the CSV and launch potential attacks such as password cracking and execute malicious commands. It has basically never been easier for an attacker to get illegal access to high-performance computing environment. Zeus botnet (phishing Trojan) was known to be hosted on virtual machine within Amazon cloud which led to Amazon's IP address range being blacklisted on spam list where good customers running email server on Amazon were rejected as well. This affects the core information security which is availability [9]. There have been instances where rouge administrators conducted nefarious activities. Countermeasures include enforcing transparency into overall information security and management practices. Moreover, a credit card fraud detection mechanism can be designed to ensure unwanted registration to the cloud. Strict penalties should be enforced to cloud violators which will minimize abuse of cloud. Also, a thorough examination of network traffic via network devices logs up to application level logs should be

continuously monitored. Furthermore, *defense-in-depth* should be used since the components include biometric verifications, antispyware, firewalls and intrusion detection [11]. Such mechanisms are based on military principles where it is very difficult to penetrate multilayered system than a single system. If a hacker gains access, *defense-in-depth* gives network engineers and administrators' time to deploy updated or new systems. A well design strategy can also identify who tried to compromise the system.

3.8 Insufficient Due-Diligence

There are hundreds of CSVs and understanding their capabilities, governance, partners, and presence/absence of redundancy and good disaster recovery in their data centers. These are actually threats if you do not perform the due diligence. When designers and architects who are unfamiliar with the cloud technologies are designing applications, unknown operational issues arise [12]. Planning for due diligence of the CSV must include *IT due-diligence checklist* such as guidance from *NIST* and *Cloud Security Alliance*. The cloud provider must setup requirement for implementing applications and service using industry standard as well perform risk assessment using qualitative and quantitative methods after certain intervals to check storage, flow and processing of data [13]. Moreover, the cloud users should consider any recent change in CSVs operating or regulatory environment, any new products adopted and other foreign operations. The cloud users should focus on how that CSV handles business continuity plan and disaster recovery plan.

3.9 Shared Technology

The three models of cloud computing (SaaS, PaaS, IaaS) is being compromised by the shared technology issue. The CSVs adopt scalable infrastructure to support multitenant environment where if one component is compromised, this exposes the risk to the entire environment which in the other hand can be said about the shared services which includes CPU caches, shared databases and shared storage. An in-depth defensive strategy should apply such as use of CPU, networking, storage, applications and user access and also monitoring should be used for destructive moves and behaviors. Nothing less than best practices of installation or configuration and monitoring for unauthorized changes should be implemented. Also, strong authentication and access control for admin access and clients should be implemented. Some other steps include SLA's for patching and vulnerability remediation and to conduct vulnerability scanning and configuration audits [7]. Moreover, if for some reason the physical server has *down-time* for maintenance or compliance reasons in the CSV's datacenter, then the guest VM's will be automatically moved to other hosts. This can be achieved through *vMotion* in *VMware* and is known as *high availability*. When moving, the right security policy and filtering capability also needs to move otherwise other VM's will gain access to your data and this can be a big security concern.

4 Conclusion

Cloud computing is a new technology which is being quickly adopted by many organizations due to the benefits it has and one of the most important aspect is the Security. We have discussed some top threats and the security techniques that can be adopted as countermeasures. While there is no full proof solution for security, the mentioned solutions can be implemented to minimize threats to some extent in the future.

References

[1] Wikipedia, "Side-channel attack" September 22, 2012. https://en.wikipedia.org/wiki/Side-channel_attack

[2] Hashizume (2013). Journal of Internet Services and applications. An analysis of security issue for cloud computing, 8-9, 2013.

[3] M. Farik, "Improving Network Security: An Alogrithm to Enforce Strong Router Password", The University of Fiji, 2014.

[4] T. Myers, "Azure Storage replication". January 9, 2015. https://azure.microsoft.com/en-us/documentation/articles/storage-redundancy/

[5] M. Cobb, "API security: How to ensure secure API use in the enterprise. " 2015. http://searchsecurity.techtarget.com/tip/API-security-How-to-ensure-secure-API-use-in-the-enterprise

[6] A. Thilakarathne, & J. Wijayanayake, "Security Challenges of Cloud Computing." International Journal of Scientific & Technology Research, 3(11), 202, 2014.

[7] V. Ashktorab & S. R. Taghizadeh, "Security Threats and Countermeasures in Cloud Computing." International Journal of Application or Innovation in Engineering & Management, 1(2), 242, October 2012.

[8] A. Venkatraman, "Azure CTO Mark Russinovich's top ten public cloud security risks." 10 October 2014. http://www.computerweekly.com/news/2240232396/How-to-mitigate-top-ten-public-cloud-security-risks-Azure-CTO-Mark-Russinovich

[9] S. Pearson, G. Yee, "Privacy and Security for Cloud Computing." London Heidelberg New York Dordrecht, London: Springer. 2013.

[10] M. Higashi, "3 Threats to Cloud Data, and How to Address Them." 3 July 2014. http://www.ciphercloud.com/blog/3-threats-cloud-data-security-address

[11] M. Rouse, "Defense in depth." 2015. http://searchsecurity.techtarget.com/definition/defense-in-depth

[12] T.T.W. Group, "The Notorious Nine: Cloud computing Top Threats in 2013", 2013. https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

[13] M. Kazim, & S. Zhu, "A Survey on Top Security Threats in Cloud Compting" International Jouornal of Advanced Computer Science and Applications, 6(3), 113, June 2015.