A survey on top security threats in cloud computing

Muhammad Kazim
University of Derby
Derby, United Kingdom

Shao Ying Zhu
University of Derby Derby,
United Kingdom

***Abstract*—Cloud computing enables the sharing of resources such as storage, network, applications and software through internet. Cloud users can lease multiple resources according to their requirements, and pay only for the services they use. However, despite all cloud benefits there are many security concerns related to hardware, virtualization, network, data and service providers that act as a significant barrier in the adoption of cloud in the IT industry. In this paper, we survey the top security concerns related to cloud computing. For each of these security threats we describe, i) how it can be used to exploit cloud components and its effect on cloud entities such as providers and users, and ii) the security solutions that must be taken to prevent these threats. These solutions include the security techniques from existing literature as well as the best security practices that must be followed by cloud administrators.**

***Keywords*—Cloud computing; Data security; Network security; Cloud service provider security**

I. Introduction

Cloud computing offers many advantages such as increased utilization of hardware resources, scalability, reduced costs, and easy deployment. As a result, all the major companies including Microsoft, Google and Amazon are using cloud computing. Moreover, the number of customers moving their data to cloud services such as iCloud, Google Drive, Dropbox, Facebook and LinkedIn are increasing every day.

Many business level security policies, standards, and practices cannot be implemented in cloud due to which different security risks arise. Although cloud security has been a focused area of research in the last decade, there are still open challenges in achieving it. To control the security risks in cloud, it is crucial for researchers, developers, service providers, and users to understand them so that they can take maximum precautions, deploy existing security techniques or develop new ones. In this paper, the top security threats for cloud computing presented by Cloud Security Alliance (CSA) [1] have been analyzed.

The CSA guide [1] presents the security threats for cloud in the order of their severity and provides controls that can be followed by the service providers to avoid these threats. However, these threats and the controls to avoid them are very mentioned specifically to meet the requirements of industry. Therefore, there is a need to survey the security threats for cloud and their solutions from the research perspective. In this paper we define these threats, describe the ways they can be launched in cloud, the possible ways to exploit these threats and their effects on cloud entities. We have comprehensively analyzed and presented the security solutions for the prevention of these threats from literature. Moreover, we have classified these security issues into three categories which are data security, network security and cloud environment security (that includes issues specific to cloud environment).

This paper is composed as follows: Section II describes the most critical threats for cloud computing and their effects on cloud entities. Section III describes the security solutions to avoid these threats, and section IV gives the conclusion of paper.

II. Threats in Cloud Computing

In this section the major threats for cloud computing are explored. These are: i) data threats including data breaches and data loss, ii) network threats including account or service hijacking, and denial of service, and iii) cloud environment specific threats including insecure interfaces and APIs, malicious insiders, abuse of cloud services, insufficient due diligence, and shared technology vulnerabilities.

A. *Data Threats*

Data is considered to be one the most important valuable resource of any organization and the number of customers shifting their data to cloud is increasing every day. Data life cycle in cloud comprises of data creation, transit, execution, storage and destruction. Data may be created in client or server in cloud, transferred in cloud through network and stored in cloud storage. When required data is shifted to execution environment where it can be processed. Data can be deleted by its owner to complete its destruction.

The biggest challenge in achieving cloud computing security is to keep data secure. The major issues that arise with the transfer of data to cloud are that the customers don't have the visibility of their data and neither do they know its location. They need to depend on the service provider to ensure that the platform is secure, and it implements necessary security properties to keep their data safe.

The data security properties that must be maintained in cloud are confidentiality, integrity, authorization, availability and privacy. However, many data issues arise due to improper handling of data by the cloud provider. The major data security threats include data breaches, data loss, unauthorized access, and integrity violations. All of these issues occur frequently on cloud data. In this paper, we focus on data breaches and data loss that are described as the two most severe threats to cloud computing by CSA [1].

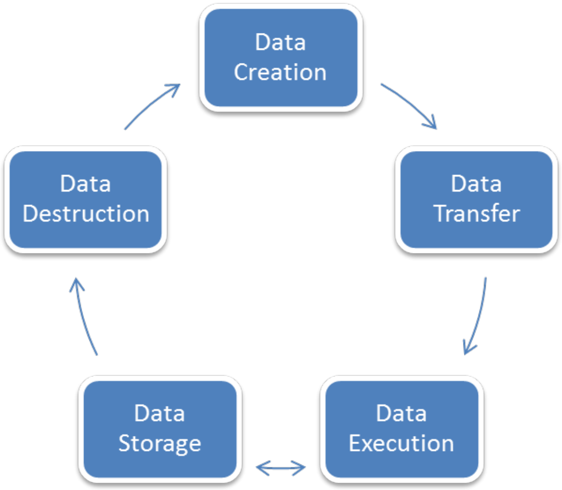

Fig. 1: Data life cycle in cloud computing

1) Data Breaches: Data breach is defined as the leakage of sensitive customer or organization data to unauthorized user. Data breach from organization can have a huge impact on its business regarding finance, trust and loss of customers. This may happen accidently due to flaws in infrastructure, application designing, operational issues, insufficiency of authentication, authorization, and audit controls [2]. Moreover, it can also occur due to other reasons such as the attacks by malicious users who have a virtual machine (VM) on the same physical system as the one they want to access in unauthorized way.

Apple's iCloud users faced a data leakage attack recently in which an attempt was made to gain access to their private data. Such attacks have also been done at other companies cloud such as Microsoft, Yahoo and Google. An example of data breach is cross VM side channel attack introduced by Y. Zhang et al., that extracts cryptographic keys of other VMs on the same system and can access their data [3].

2) Data Loss: Data loss is the second most important issue related to cloud security. Like data breach, data loss is a sensitive matter for any organization and can have a devastating effect on its business. Data loss mostly occurs due to malicious attackers, data deletion, data corruption, loss of data encryption key, faults in storage system, or natural disasters. 44 percent of cloud service providers have faced brute force attacks in 2013 that resulted in data loss and data leakage [4]. Similarly, malware attacks have also been targeted at cloud applications resulting in data destruction.

B. Network Threats

Network plays an important part in deciding how efficiently the cloud services operate and communicate with users. In developing most cloud solutions, network security is not considered as an important factor by some organizations. Not having enough network security creates attacks vectors for the malicious users and outsiders resulting in different network threats. Most critical network threats in cloud are account or service hijacking, and denial of service attacks.

1) Account or Service Hijacking: Account hijacking involves the stealing of user credentials to get an access to his account, data or other computing services. These stolen credentials can be used to access and compromise cloud services. The network attacks including phishing, fraud, Cross Site Scripting (XSS), botnets, and software vulnerabilities such as buffer overflow result in account or service hijacking. This can lead to the compromise of user privacy as the attacker can eavesdrop on all his operations, modify data, and redirect his network traffic. 1n 2009 a legitimate service was purchased from Amazon's EC2, and compromised to act as Zeus botnet [5].

2) Denial of Service: Denial of Service (DOS) attacks are done to prevent the legitimate users from accessing cloud network, storage, data, and other services. DOS attacks have been on rise in cloud computing in past 5 years and 81 percent customers consider it as a significant threat in cloud [1]. They are usually done by compromising a service that can be used to consume most cloud resources such as computation power, memory, and network bandwidth. This causes a delay in cloud operations, and sometimes cloud is unable to respond to other users and services.

Distributed Denial of Service (DDOS) attack is a form of DOS attacks in which multiple network sources are used by the attacker to send a large number of requests to the cloud for consuming its resources. It can be launched by exploiting the vulnerabilities in web server, databases, and applications resulting in unavailability of resources.

C. Cloud environment specific threats

Cloud service providers are largely responsible for controlling the cloud environment. However, a survey report by Alert Logic [4] shows that almost 50 percent of the cloud users consider service provider issues as a major threat in cloud computing. Apart from service provider threats, some threats are specific to cloud computing such as providing insecure interfaces and APIs to users, malicious cloud users, shared technology vulnerabilities, misuse of cloud services, and insufficient due diligence by companies before moving to cloud.

1) Insecure Interfaces and APIs: Application Programming Interface (API) is a set of protocols and standards that define the communication between software applications through internet. Cloud APIs are used at all the infrastructure, platform and software service levels to communicate with other services. Infrastructure as a Service (IaaS) APIs are used to access and manage infrastructure resources including network and VMs, Platform as a Service (PaaS) APIs provide access to the cloud services such as storage and Software as a Service (SaaS) APIs connect software applications with the cloud infrastructure. The security of various cloud services depends on the APIs security. Weak set of APIs and interfaces can result in many security issues in cloud. Cloud providers generally offer their APIs to third party to give services to customers. However, weak APIs can lead to the third party having access to security keys and critical information in cloud. With the security keys, the encrypted customer data in cloud can be read resulting in loss of data integrity, confidentiality and availability. Moreover, authentication and access control principles can also be violated through insecure APIs.

2) Malicious Insiders: A malicious insider is someone who is an employee in the cloud organization, or a business partner with an access to cloud network, applications, services, or data, and misuses his access to do unprivileged activities. Cloud administrators are responsible for managing, governing, and maintaining the complete environment. They have access to most data and resources, and might end up using their access to leak that data. Other categories of malicious insiders involve hobbyist hackers who are administrators that want to get unauthorized sensitive information just for fun, and corporate espionage that involves stealing secret information of business for corporate purposes that might be sponsored by national governments.

3) Abuse of Cloud Services: The term abuse of cloud services refers to the misuse of cloud services by the consumers. It is mostly used to describe the actions of cloud users that are illegal, unethical, or violate their contract with the service provider. Abusing of cloud services was considered to be the most critical cloud threat in 2010 [2], and different measures were taken to prevent it. However, 84 percent of cloud users still consider it as a relevant threat [1]. Research has shown that some cloud providers are unable to detect attacks launched from their networks, due to which they are unable to generate alerts or block any attacks. The abuse of cloud services is a more serious threat to the service provider than service users. For instance, the use of cloud network addresses for spam by malicious users has resulted in blacklisting of all network addresses, thus the service provider must ensure all possible measures for preventing these threats.

Over the years, different attacks have been launched through cloud by the malicious users. For example, Amazon's EC2 services were used as a command and control servers to launch Zeus botnet in 2009 [6]. Famous cloud services such as Twitter, Google and Facebook as a command and control servers for launching Trojans and botnets. Other attacks that have been launched using cloud are brute force for password cracking of encryption, phishing, performing DOS attack against a web service at specific host, Cross Site Scripting and SQL injection attacks.

4) Insufficient Due Diligence: The term due diligence refers to individuals or customers having the complete information for assessments of risks associate with a business prior to using its services. Cloud computing offers exciting opportunities of unlimited computing resources, and fast access due which number of businesses shift to cloud without assessing the risks associated with it.

Due to the complex architecture of cloud, some of organization security policies cannot be applied using cloud. Moreover, the cloud customers have no idea about the internal security procedures, auditing, logging, data storage, data access which results in creating unknown risk profiles in cloud. In some cases, the developers and designers of applications maybe unaware of their effects from deployment on cloud that can result in operational and architectural issues.

5) Shared Technology Vulnerabilities: Cloud computing offers the provisioning of services by sharing of infrastructure, platform and software. However, different components such as CPUs, and GPUs may not offer cloud security requirements such as perfect isolation. Moreover, some applications may be designed without using trusted computing practices due to which threats of shared technology arise that can be exploited in multiple ways. In recent years, shared technology vulnerabilities have been used by attackers to launch attacks on cloud. One such attack is gaining access to the hypervisor to run malicious code, get unauthorized access to the cloud resources, VMs, and customers data.

Xen platform is an open source solution used to offer cloud services. Xen hypervisors code creates local privilege escalation (in which a user can have rights of another user) vulnerability that can be launch guest to host VM escape attack. Later, Xen updated the code base of its hypervisor to fix that vulnerability. Other companies such as Microsoft, Oracle and SUSE Linux that were based on Xen also released updates of their software to fix the local privilege escalation vulnerability. Similarly, a report released in 2009 [7] showed the usage of VMware to run code from guests to hosts showing the possible ways to launch attacks.

III. Security techniques for threats protection

In this section the security methods to avoid the exploitation of threats mentioned in section II have been discussed. We describe the implementation of these security techniques at different levels to secure cloud from threats.

A. Data Security

1) Protection from Data Breaches: Various security measures and techniques have been proposed to avoid the data breach in cloud. One of these is to encrypt data before storage on cloud, and in the network. This will need efficient key management algorithm, and the protection of key in cloud. Some measures that must be taken to avoid data breaches in cloud are to implement proper isolation among VMs to prevent information leakage, implement proper access controls to prevent unauthorized access, and to make a risk assessment of the cloud environment to know the storage of sensitive data and its transmission between various services and networks.

Considerable amount of research has been carried out for the protection of data in cloud storage. CloudProof [8] is a system that can be built on top of existing cloud storages like Amazon S3 and Azure blob to ensure data integrity and confidentiality using encryption. To secure data in cloud storage attributed based encryption can be used to encrypt data with a specific access control policy before storage. Therefore, only the users with access attributes and keys can access the data [9]. Another technique to protect data in cloud involves using scalable and fine grained data access control [10]. In this scheme, access policies are defined based on the data attributes. Moreover, to overcome the computational overhead caused by fine grained access control, most computation tasks can be handed over to untrusted commodity cloud with disclosing data. This is achieved by combining techniques of attribute-based encryption, proxy re-encryption, and lazy re-encryption.

2) Protection from Data Loss: To prevent data loss in cloud different security measures can be adopted. One of the most important measure is maintain backup of all data in cloud which can be accessed in case of data loss. However, data backup must also be protected to maintain the security properties of data such as integrity and confidentiality. Different data loss prevention (DLP) mechanisms have been proposed in research and academics for the prevention of data loss in network, processing, and storage. Many companies including Symantec, McAfee, and Cisco have also developed solutions to implement data loss prevention across storage systems, networks and end points.

R Chow et al. proposed the usage of Trusted Computing to provide data security. A trusted server can monitor the functions performed on data by cloud server and provide the complete audit report to data owner. In this way, the data owner can be sure that the data access policies have not been violated [11]. Tomoyoshi T. et al. proposed a system to protect moving data of a company inside a USB even if it is lost. They also describe the protection of document in its complete life cycle and avoiding data loss through emails [12].

B. Network Security

1) Protection from Account or Service Hijacking: Account or service hijacking can be avoided by adopting different security features on cloud network. These include employing intrusion detection systems (IDS) in cloud to monitor network traffic and nodes for detecting malicious activities. Intrusion detection and other network security systems must be designed by considering the cloud efficiency, compatibility and virtualization based context [13]. An IDS system for cloud was designed by combining system level virtualization and virtual machine monitor (responsible for managing VMs) techniques [14]. In this architecture, the IDSs are based on VMs and the sensor connectors on Snort which is a well-known IDS [15]. VM status and their workload are monitored by IDS and they can be started, stopped and recovered at any time by management system of IDS.

Identity and access management should also be implemented properly to avoid access to credentials. To avoid account hijacking threats, multi factor authentication for remote access using at least two credentials can be used. A technique that uses multi-level authentication at different levels through passwords was made to access the cloud services. First the user is authenticated by the cloud access password and in the next level the service access password of user is verified [16]. Moreover, user access to cloud services and applications should be approved by cloud management. The auditing of all the privileged activities of the user along with information security events generated from it should also be done to avoid these threats [17].

2) Protection from Denial of Service: To avoid DOS attacks it is important to identify and implement all the basic security requirements of cloud network, applications, databases, and other services. Applications should be tested after designing to verify that they have no loop holes that can be exploited by the attackers.

The DDOS attacks can be prevented by having extra network bandwidth, using IDS that verify network requests before reaching cloud server, and maintaining a backup of IP pools for urgent cases. Industrial solutions to prevent DDOS attacks have also been provided by different vendors. C. Jin et al. [18] proposed a technique named hop count filtering that can be used to filter spoofed IP packets, and helps in decreasing DOS attacks by 90 percent. Another technique for securing cloud from DDOS involves using intrusion detection system in VM [19]. In this scheme when an IDS detects an abnormal increase in inbound traffic, the targeted applications are transferred to VMs hosted on another data center.

C. Cloud Environment Security

1) Protection from Insecure Interfaces and APIs: To protect the cloud from insecure API threats it is important for the developers to design these APIs by following the principles of trusted computing. Cloud providers must also ensure that all the all the APIs implemented in cloud are designed securely, and check them before deployment for possible flaws. Strong authentication mechanisms and access controls must also be implemented to secure data and services from insecure interfaces and APIs. The Open Web Application Security Project (OWASP) [20] provides standards and guidelines to develop secure applications that can help in avoiding such application threats. Moreover, it is the responsibility of customers to analyze the interfaces and APIs of cloud provider before moving their data to cloud.

2) Protection from Malicious Insiders: The protection from these threats can be achieved by limiting the hardware and infrastructure access only to the authorized personnel. The service provider must implement strong access control, and segregation of duties in the management layer to restrict administrator access to only his authorized data and software. Auditing on the employees should also be implemented to check for their suspicious behaviour. Moreover, the employee behaviour requirements should be made part of legal contract, and action should be taken against anyone involved in malicious activities [17]. To prevent data from malicious insiders encryption can also be implemented in storage, and public networks.

3) Protection from Abuse of Cloud Services: The implementation of strict initial registration and validation processes can help in identifying malicious consumers. The policies for the protection of important assets of organization must also be made part of the service level agreement (SLA) between user and service provider. This will familiarize user about the possible legal actions that can be conducted against him in case he violates the agreement. The Service Level Agreement definition language (SLAng) [21] enables to provide features for SLA monitoring, enforcement and validation. Moreover, the network monitoring should be comprehensive for detecting malicious packets and all the updated security devices in network should be installed.

4) Protection from Insufficient Due Diligence: It is important for organizations to fully understand the scope of risks associated with cloud before shifting their business and critical assets such as data to it. The service providers must disclose the applicable logs, infrastructure such as firewall to consumers to take measures for securing their applications and data [17]. Moreover, the provider must setup requirements for implementing cloud applications, and services using industry standards. Cloud provider should also perform risk assessment using qualitative and quantitative methods after certain intervals to check the storage, flow, and processing of data.

5) Protection from Shared Technology Vulnerabilities: In cloud architecture, hypervisor is responsible for mediating interactions of virtual machines and the physical hardware. Therefore, hypervisor must be secured to ensure proper functioning of other virtualization components, and implementing isolation between VMs. Moreover, to avoid shared technology threats in cloud a strategy must be developed and implemented for all the service models that includes infrastructure, platform, software, and user security. The baseline requirements for all cloud components must be created, and employed in design of cloud architecture. The service provider should also monitor the vulnerabilities in the cloud environment, and release patches to fix those vulnerabilities regularly [17].

IV. CONCLUSION

Cloud computing is getting widely adopted in businesses around the world. However, there are different security issues associated with it. In order to maintain the trust of customers, security should be considered as an integral part of cloud. In this paper we have focused on most severe threats on cloud computing that are considered relevant by most users and businesses. We have divided these threats into categories of data threats, networks threats, and cloud environment specific threats. The impact of these threats on cloud users and providers has been illustrated in the paper. Moreover, we also discuss the security techniques that can be adopted to avoid these threats.

REFERENCES

[1] T. T. W. Group *et al.*, "The notorious nine: cloud computing top threats in 2013," *Cloud Security Alliance*, 2013.

[2] C. S. Alliance, "Top threats to cloud computing v1. 0," *Cloud Security Alliance, USA*, 2010.

[3] Y. Zhang, A. Juels, M. K. Reiter, and T. Ristenpart, "Cross-vm side channels and their use to extract private keys," in *Proceedings of the 2012 ACM conference on Computer and communications security*. ACM, 2012, pp. 305–316.

[4] "Cloud security report spring 2014," https://www.alertlogic.com/resources/cloud-security-report//, last Accessed: 2014-11-08.

[5] "Zeus bot found using amazon's ec2 as c and c server," http://www.theregister.co.uk/2009/12/09/amazon_ec2_bot_control_channel//, last Accessed: 2014-11-15.

[6] "Amazon ec2 cloud service hit by botnet, outage," http://www.cnet.com/uk/news/amazon-ec2-cloud-service-hit-by-botnet-outage/, last Accessed: 2014-11-15.

[7] K. Kortchinsky, "Cloudburst: A vmware guest to host escape story," *Black Hat USA*, 2009.

[8] R. A. Popa, J. R. Lorch, D. Molnar, H. J. Wang, and L. Zhuang, "Enabling security in cloud storage slas with cloudproof." in *USENIX Annual Technical Conference*, vol. 242, 2011.

[9] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 25, no. 2, pp. 384–394, 2014.

[10] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *INFOCOM, 2010 Proceedings IEEE*. Ieee, 2010, pp. 1–9.

[11] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, "Controlling data in the cloud: outsourcing computation without outsourcing control," in *Proceedings of the 2009 ACM workshop on Cloud computing security*. ACM, 2009, pp. 85–90.

[12] T. Takebayashi, H. Tsuda, T. Hasebe, and R. Masuoka, "Data loss prevention technologies," *Fujitsu Scientific and Technical Journal*, vol. 46, no. 1, pp. 47–55, 2010.

[13] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in cloud," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 42–57, 2013.

[14] S. Roschke, F. Cheng, and C. Meinel, "Intrusion detection in the cloud," in *Dependable, Autonomic and Secure Computing, 2009. DASC'09. Eighth IEEE International Conference on*. IEEE, 2009, pp. 729–734.

[15] "Snort," https://www.snort.org//, last Accessed: 2015-01-29.

[16] H. Dinesha and V. Agrawal, "Multi-level authentication technique for accessing cloud services," in *Computing, Communication and Applications (ICCCA), 2012 International Conference on*. IEEE, 2012, pp. 1–4.

[17] "Cloud controls matrix (ccm), cloud security alliance," https://cloudsecurityalliance.org/research/ccm/, last Accessed: 2014-12-02.

[18] C. Jin, H. Wang, and K. G. Shin, "Hop-count filtering: an effective defense against spoofed ddos traffic," in *Proceedings of the 10th ACM conference on Computer and communications security*. ACM, 2003, pp. 30–41.

[19] A. Bakshi and B. Yogesh, "Securing cloud from ddos attacks using intrusion detection system in virtual machine," in *Communication Software and Networks, 2010. ICCSN'10. Second International Conference on*. IEEE, 2010, pp. 260–264.

[20] D. Fox, "Open web application security project," *Datenschutz und Datensicherheit-DuD*, vol. 30, no. 10, pp. 636–636, 2006.

[21] A. Al Falasi and M. A. Serhani, "A framework for sla-based cloud services verification and composition," in *Innovations in Information Technology (IIT), 2011 International Conference on*. IEEE, 2011, pp. 287–292.