International Journal of Scientific & Engineering Research, Volume 4, Issue 3, March -2013
ISSN 2229-5518

A Survey on Security Threats and Vulnerabilities In Cloud Computing

W.Sharon Inbarani, C.Kumar Charlie Paul, W.Andrew Jerome Jeevakumar

Abstract— Cloud computing is a distributed computing paradigm capable of providing agile IT services to individual users and organizations. Cloud computing is a technology which will facilitate companies or organizations to host their services without worrying about IT infrastructure and other supporting services. Cloud computing providers can build large data centers at low cost due to their expertise in organizing and provisioning computational resources. Cloud security has emerged as arguably the most significant barrier to faster and more widespread adoption of cloud computing. Indeed, cloud computing suffers from threats and vulnerabilities which hinders the users from trusting it. In this paper, we explore the vulnerabilities and threats of cloud storage one of the domains of cloud computing that affects the different cloud service model.

Index Terms— Cloud computing, Eavesdropping, Exploitation, Malicious. Threat, Threshold cryptography, Vulnerabilities

1 Introduction

CLOUD computing is the promising utility computing, where applications and services are moving into the internet called as “cloud”. The cloud users store their resources into the cloud servers and pay for the amount of time they use the services. The cloud customers enjoy the high quality networks, applications, servers and services from a shared pool of configurable computing resources [4]. Many corporations including Amazon, Google, SUN, IBM, Oracle, Intel, HP, Windows Azure have invested in cloud computing and offers cloud-based solutions. The primary service models deployed by cloud computing services in terms of business models can be classified into three categories. They are Infrastructure as a Service : IaaS, Platform as a Service : PaaS, and Software as a Service : SaaS [7]. Cloud has advantages in offering more scalable, fault- tolerant services, flexibility, business continuity and access to automatic updates. Cloud computing can provide infinite computing resources on demand due to high scalability in nature. This eliminates the needs for cloud service providers to plan ahead for hardware provisioning [6]. The four deployments of the cloud are private cloud, public cloud, community cloud, and hybrid cloud.

According to NIST cloud computing exhibits five essential characteristics. [10].

A. On Demand Self Service

A consumer can provision computing resources, such as server time, email, applications, network storage, without requiring assistance from the service provider.

B. Broad Network Access

The resources which are available over the network can be accessed through a standard mechanisms that promote use by heterogeneous thin or thick client platforms.

C. Resource Pooling

The providers computing resources such as processing, memory, and network bandwidth are pooled to serve multiple consumers. This can be achieved with a multi - tenant model. Higher application density and higher resource utilization can be achieved by resource pooling.

D. Rapid Elasticity

Capabilities can be rapidly and elastically provisioned, in some cases automatically, to scale rapidly outward and inward commensurate with demand [10].

E. Measured Service

The cloud computing system offers the metering capability, which automatically controls and optimize resource use. The cloud computing resource usage can be measured, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

2 CLOUD COMPUTING THREATS

Security and privacy are the challenges associated with cloud computing, which relates to storing and securing data, monitoring the use of the cloud by the service provider. New threats avenues are introduced, when an organization moves their critical data and applications to a cloud storage servers and new approaches for securing data in the cloud must be implemented. Top seven security threats to Cloud computing discovered by “Cloud Security Alliance (CSA)” are [9]

2.1 Abuse and Nefarious use of Cloud Computing

Abuse and Nefarious use of cloud computing is the top threat identified by the CSA [9]. The cloud users are provided with unlimited bandwidth, storage capacity, free limited periods by the cloud service providers This gives an opportunity for the hackers to access the cloud, such that passwords are cracked and decoded. This threat leads to launch potential attack points and malicious commands are executed. The attackers upload malware to thousands of computers and use the power of cloud infrastructure to attack other machines in the network.

The remedies suggested by CSA to lessen this threat are:

1. Stricter initial registration and validation processes.
2. Enhanced credit card fraud monitoring and coordina-

tion.
3. Comprehensive introspection of customer network traffic.
4. Monitoring public blacklists for one's own network blocks.

2.2 Insecure Interfaces and APIs

Cloud computing providers offer a set of software interfaces or APIs that cloud users can use to manage and interact with cloud services. These interfaces are used to perform provisioning, orchestration and monitoring of the processes running in a cloud environment. The cloud services security and availability depends upon the security of the APIs. The features of APIs are authentication, access control, encryption and activity monitoring. The APIs must be designed both accidental and malicious attempts to avoid threats. To offer value-added services to their customers, organization and third party build upon these interfaces.

The remedies suggested by CSA to lessen this threat are:

1. Analyze the security model of cloud provider interfaces.
2. Ensure strong authentication and access control are implemented in concert with encrypted transmission.
3. Understand the dependency chain associated with the API.

2.3 Malicious Insiders

The threat of a malicious insider is a well known to most organizations. Malicious insider can steal the confidential data of cloud users. This threat can break the trust of cloud users on the provider. A malicious insider can easily obtain passwords, cryptographic keys and files. These attacks may involve various types of fraud, damage or theft of information and misuse of IT resources. Some of the ways a malicious insider can affect an operation are, brand damage, financial impact, and productivity losses. The threat of malicious attacks has increased due to lack of transparency in cloud provider's processes and procedures [8]. It means that a provider may not reveal how it grants employees access to physical and virtual assets, how it monitors these employees, or how it analyses and reports on policy compliances. There is often little or no visibility into the hiring standards and practices for cloud employees. This kind of situation creates an opportunity for an adversary, hackers or other cloud intruders to steal confidential information or to take control over the cloud. The level of access granted could enable attackers to collect confidential data or to gain complete control over the cloud services with little or no risk of detection.

The remedies suggested by CSA to lessen this threat are:

1. Enforce strict supply chain management and conduct a comprehensive supplier assessment.
2. Specify human resource requirements as part of legal contracts.
3. Require transparency into overall information security and management practices, as well as compliance reporting.
4. Determine security breach notification processes.

2.4 Shared technology issues

IaaS vendor shares the infrastructure to deliver their services. The CPU caches, GPU etc. are the underlying components make up this infrastructure. These infrastructures are not designed to offer strong isolation properties for a multi-tenant architecture. To address this issue, a Virtualization hypervisor mediates access between guest operating systems and the physical compute resources. Hypervisors have exhibited imperfection which has enabled guest operating systems to gain inappropriate levels of control or influence on the underlying platform. Strong compartmentalization should be employed to ensure that individual customers do not clash the operations of other tenants running on the same cloud provider. Customers should not have access to any other tenant's actual or residual data, network traffic, etc.

The remedies suggested by CSA to lessen this threat are:

1. Implement security best practices for installation/configuration.
2. Monitor environment for unauthorized changes/activity.
3. Promote strong authentication and access control for administrative access and operations.
4. Enforce service level agreements for patching and vulnerability remediation.
5. Conduct vulnerability scanning and configuration audits.

2.5 Data Loss and Leakage

Data loss in cloud occurs due to operational failures, unreliable data storage and inconsistent use of encryption keys. Operational failure occurs due to deletion or alteration of records without a backup of the original content that can take place intentionally or unintentionally. Unreliable data storage occurs due to saving of data on unreliable media that will be unrecoverable if data is lost. The inconsistent use of encryption keys will result into loss and unauthorized accesses of data by illegal users. This leads to the destruction of sensitive and confidential information. The unauthorized parties must be prevented from gaining access to sensitive data. Data loss will have a destructive impact on a business. The data loss could significantly impact employee, partner, and customer morale and trust which leads to the damage of brand and reputation. Depending upon the data that is lost or leaked, there might be compliance violations and legal ramifications.

The remedies suggested by CSA to lessen this threat are:

1. Implement strong API access control.
2. Encrypt and protect integrity of data in transit.
3. Analyzes data protection at both design and run time.
4. Implement strong key generation, storage and man-

- *W. Sharon Inbarani is currently pursuing a masters degree program in Computer Science and Engineering in A.S.L Pauls College of Engineering and Technology, Coimbatore, India.*
- *Dr. Kumar Charlie Paul is working as a principal in A.S.L Pauls College of Engineering and Technology, Coimbatore, India.*
- W. Andrew Jerome Jeevakumar is currently working as a junior project engineer in Value Addition Private Limited, Sharjah, UAE.

agement, and destruction practices.

5. Contractually demand providers wipe persistent media before it is released into the pool.
6. Contractually specifies provider backup and retention strategies.

2.6 Account and Service Hijacking

Account ans Service Hijacking is one of the major threats in cloud computing. It refers to unauthorized access of a user's credentials by attackers, such as fishing, denial of service attacks, the man in the middle attack, fraud, and exploitation of software vulnerabilities. The attacker gains the access to a user's credentials, such that the user's data will be manipulated, eavesdropping occurs, return falsified information, and clients will be redirected to illegitimate sites. The user's account will become a new base for the attacker which leads to subsequent attacks. The user credentials are stolen by the attacker which leads to top threat. With the use of stolen credentials the attackers can access the critical areas of cloud computing services. The confidentiality, integrity and availability of cloud services are compromised.

The remedies suggested by CSA to lessen this threat are:

1. Enforce strict supply chain management and conduct a comprehensive supplier assessment.
2. Specify human resource requirements as part of legal contracts.
3. Require transparency into overall information security and management practices, as well as compliance reporting.
4. Determine security breach notification processes.

2.7 Unknown risk profile

One of the main tenants in cloud computing is the reduction of hardware and software ownership and maintenance so that it allows the companies to focus on their core business strength. This leads to operational and financial benefits. When adopting cloud services, the internal security procedures, configuration hardening, patching, auditing, and logging should be taken into concern. The important factors for estimating the organization security postures are versions of software, code updates, security practices, vulnerability profiles, intrusion attempts, and security design.

The remedies suggested by CSA to lessen this threat are:

1. Enforce strict supply chain management and conduct a comprehensive supplier assessment.
2. Specify human resource requirements as part of legal contracts.
3. Require transparency into overall information security and management practices, as well as compliance reporting.
4. Determine security breach notification processes.

3 CLOUD COMPUTING VULNERABILITIES

Security vulnerabilities are predominant across all facets of cloud computing. The internet is always a ground of attack for malicious activities as it is easily accessible. Vulnerabilities allows the attacker to reduce the systems information assurance. Cloud computing can be accessed through the internet and the resources which are stored in the cloud are valuable. Several significant strategies should be followed when an organization is ready to move their valuable data to a cloud computing environment. In the following section, several significant vulnerabilities are described as follows.

3.1 Byzantine Failure

Byzantine failure is an arbitrary fault which occurs in cloud storage . This failure occurs due to a software bug, a hardware malfunction, or a malicious attack. In cloud storage many nodes participate to complete an activity. Many redundant servers and multiple users are involved in cloud storage system accessing the single source. Threshold cryptography can be implemented to ensure that the system is tolerant of Byzantine failure [3].

3.2 Virtual machine Based Rootkit

Virtual Machine Based Rootkit is one of the important aspect of cloud computing where the operating system, user applications, will run in a virtualized environment. Hence any security applications which run on the original operating system will run in a virtualized environment. Virtual Machine Based Rootkit is the new type of malware, which installs underneath the operating system layer and hoist the operating system to a virtual machine. It is very difficult to detect VMBR's state of the software running on the operating system. VMBR can be detected by controlling the layer beneath it with the help of secure hardware or bootable media.

3.3 Session Riding and Session Hijacking

In session riding , commands will be sent to the web applications on behalf of the targeted user by sending the user an email or tricking the user to into visiting a specially crafted website. Session riding deletes user data, execute online transactions such as bids or orders, triggers commands inside an intranet from the internet, system and network configurations are changed, sends spam and even opens the firewall [11]. In a network , session hijacking refers to a security attack on a user session to gain unauthorized access to the information and services residing on a computer system. Session hijacking are intrinsic to web application technologies in which it weakens the web application structure providing a way for hackers to accomplish a wide variety of malicious activities.

3.4 Internet Protocol Vulnerabilities

Cloud services are accessed through the network using standard protocols. The network is the internet which can be considered as an untrusted network. The man in the middle attack is one of the vulnerabilities which occurs in Internet Protocols. The man in the middle attack is one of the masquerade attack in cloud computing. The cyber criminals funnel communication between a consumer and an organization through a fake website. Into these types of attacks the attackers get into the middle of the user and the organization and eavesdrop on the data goes back and forth.

3.5 Injection Vulnerabilities

Injection vulnerabilities are exploited in cloud computing by manipulating input to an application such that parts of the input are interpreted and executed as the code against the injections of the programmer [2]. Some of the examples of injection vulnerabilities are SQL injection, Command injection, cross-site scripting. SQL injection is a vulnerability which injects malicious database scripts when user inputs are not properly validated. The SQL code will be erroneously executed in the database backend. SQL injection is very dangerous because it is used to change values of multiple records and even delete the entire table [5]. Command injection injects and execute command specified by the attacker in the vulnerable application. This type of injection occurs due to the lack of correct input data validation, which can be manipulated by the attacker. Cross side scripting is another vulnerability, in which the input contains javascript code which are erroneously executed by a victim's browser.

3.6 Resource Exhausion

The resource exhaustion vulnerability occurs due to the consumption or allocation of any resources in an unnecessary way. Resource exhaustion causes denial of service attacks. It can be caused due to bad design, inefficient utilization of resources on the service side, and resource leakage [1]. Resource exhaustion can be monitored by using black box testing. Predator methodology is used to predict resource exhaustion vulnerability.

4 Conclusion

Cloud computing eliminates the worries of maintaining and securing IT infrastructure and increase speed and agility of the software development life cycle. All the cloud computing activities purely depend on the Internet through which client connects to the cloud service provider. There are different threats and vulnerabilities that affects the cloud storage systems. It is necessary to develop and design security techniques to protect the data stored in a cloud environment. This survey helps in understanding various threats and vulnerabilities in cloud computing. Indeed, many current developments in cloud computing such as the development of security metrics for cloud computing, certification schemes for cloud computing, or the move towards full-featured virtualized network components directly address control challenges by enabling the use of such tried and tested controls for cloud computing.

References

[1] Antunes, J., N. Neves, et al., "Detection and Prediction of Resource-Exhaustion Vulnerabilities", ISSRE 2008, pp. 87-96.

[2] Bernd Grobauer, Tobias Walloschek, Elmar Stöcker, "Understanding Cloud Computing Vulnerabilities,"in proc. Of IEEE, March-April 2011, pp. 50-57.

[3] Cachin.C and S. Tessaro. "Optimal resilience for erasure-coded Byzantine distributed storage," *Distributed Computing* , 2005, pp. 497-498.

[4] Cong Wang, Qian Wang, Kui Ren, Wenjing Lou "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in *Proc. IEEE INFOCOM,* March 2010, pp. 1-9.

[5] Fu, X. and K. Qian , "SAFELI: SQL injection scanner using symbolic execution", Proceedings of the 2008 workshop on Testing, analysis, and verification of web services and applications , 2008, pp. 34-39.

[6] Hsiao–Ying Lin and Wen-Guey Tzeng, "A Secure Decentralized Erasure Code for Distributed Network Storage*," IEEE Trans. Parallel and Distributed Systems*, Nov. 2010, pp. 1586-1594.

[7] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, "On technical Security Issues in Cloud Computing,"in *Proc. of IEEE International Conference on Cloud Computing* , 2009, pp. 109-116.

[8] Mervat Adib Bamiah, Sarfraz Nawaz Brohi, " Seven Deadly Threats and Vulnerabilities in Cloud Computing," *IJAEST,*2011, pp. 87-90.

[9] Security Guidance for Critical Areas of Focus in Cloud Computing, April2009.DOI=http://www.cloudsecurityalliance.org/topthreats/csathreats.

[10] The National Institute of Standards and Technology (NIST), Information Technology Laboratory definition of Cloud Computing by Peter Mell and Tim Grance, version 15, October 2009.

[11] T. Schreiber, "Session Riding a Widespread Vulnerability in Today's WebApplications"[Online],Available:http://www.securenet.de/papers/Session_Riding.pdf, white paper, 2004.