A REVIEW ON DATA PRIVACY PROTECTION AND TYPES OF ATTACKS IN CLOUD COMPUTING

Satheeshkumar R.[1] and Kannamal N.[2]
[1]Department. of Information Technology, Hindusthan College of Engineering and Technology, Coimbatore, Tamilnadu, India
[2]Department of Information Technology, Surya Engineering College, Perundurai, Erode, Tamilnadu, India
E-Mail: satheeshpkd@gmail.com

ABSTRACT

In recent years, lots of organizations have adopted their systems for enabling cloud based computing to provide scalable, virtualized on-demand privilege to a shared pool of computing resources such as networks, servers, storage, applications and services. Mainly cloud computing technology enables users/enterprises to eliminate the requirements for setting up of expensive computing infrastructure and reduces systems' operating costs. So, this type of technology was used by more number of end users. On the other hand, existing invulnerability deficiencies and vulnerabilities of underlying technologies can leave an open door for intrusions. Therefore, cloud computing providers need to protect their users' sensitive data from insider or outsider attacks by installing an intrusion detection and prevention system. In this paper, it was aimed to define different attack types, which affect the availability, confidentiality and integrity of resources and services in cloud computing environment. Additionally, the paper also introduces related interrupt detection models to identify and prevent these types of attacks.

Keywords: cloud computing, SaaS, IaaS PaaS.

1. INTRODUCTION

Cloud computing was currently one the most hyped IT innovations. Most IT companies announce to plan or (suddenly) already have IT products according to the cloud computing paradigm. In the nearest future, we can expect to see a lot of new invulnerability exploitation events around cloud computing providers and users, which will shape the cloud computing invulnerability research directions for the next decade. Hence, we have seen a rapid evolution of a cloud computing invulnerability discipline, with ongoing efforts to cope with the idiosyncratic requirements and capabilities regarding privacy and invulnerability issues that this new paradigm raises. In line with these developments, the authors closely watch cloud computing invulnerability on a very technical level, focusing primarily on attacks and hacking attempts related to cloud computing providers and systems. Here, as Lowis and Accorsi pointed out lately, the specific invulnerability threats and vulnerabilities of services and service-oriented architectures require new taxonomies and classification criteria, so do attacks on cloud computing framework [1]. In this paper, we try to anticipate the classes of vulnerabilities that will arise from the cloud computing paradigm, and we give preliminary attack taxonomy for these, based on the notion of attack surfaces.

2. CLOUD COMPUTING

Pervasive computing was first defined conceptually as "previligeibility of data with technological opportunities has to be realized with a continuous and an invisible way" by Mark Weiser who was a Xerox Palo Alto Research Center (PARC) Incorporated researcher with an inspiration from Philip K. Dick's Ubik novel [2, 3]. In Ubik, all objective entities were communicating each other as a smart entity. This communication occurs dependently with all factors in the environment. Communication networks allow data privilege perpetually independent from the environment. A real-time and location independent interactive communication environment was started to be used by inclusion of pervasive computing in daily life [4]. Cloud computing was an interactive communication model that was constituted in more than one place nonexistent, easy to use, can be privileged whenever user needs, consist of configurable computing resources and needs minimal effort to achieve maintainability [5]. Nowadays cloud computing users were using services that they need from providers' computing resources and charged as they profited [6]. Cloud computing has many definitions in different resources, which were similar to each other. As a summary, cloud computing can be defined as today's computing technology that has time and location independent services, shaped with user's needs, has a minimum effort to maintain and charged as the service usage provider and consumer, and also it enables consumers can privilege to the services over communication infrastructure and other devices such as desktops, laptops or any mobile devices. Distribution of the cloud services can be realized via network and communication agents, which have high storage capacity opportunities.

Service models in cloud computing

About the services, which were served over cloud computing systems there was a definition as anything as aService (XaaS). The word anything defines the service, and it can take part as the type of the service like; Communication as a Service (CaaS), Network as a Service (NaaS) or Monitoring as a Service (MaaS). However, there were three fundamental service types to describe and define the service contents. They were infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) [5]. These three main service models/actors of the cloud computing were shown in Figure-1 and detailed as follows.

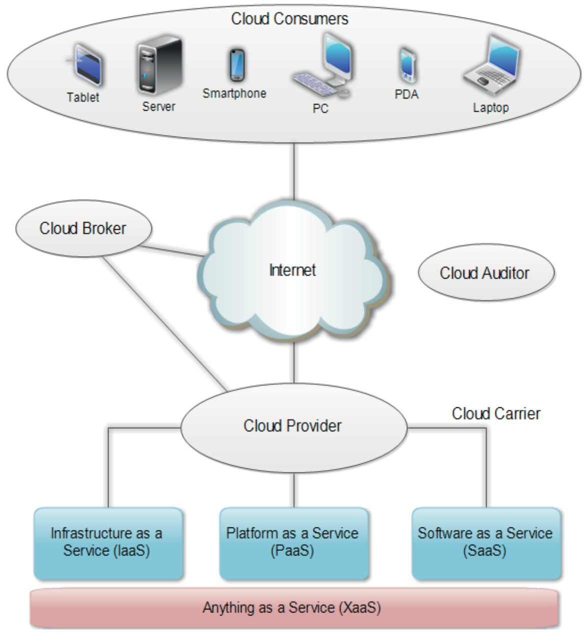
Cloud Consumers
Tablet
Server
Smartphone
PC
PDA
Laptop
Cloud Broker
Internet
Cloud Auditor
Cloud Provider
Cloud Carrier
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)
Software as a Service (SaaS)
Anything as a Service (XaaS)

Figure-1. Service models and actors in cloud computing.

Infrastructure as a service (IaaS): With this ability, users can privilege processing power, storage area, network and other computing resources through opportunity and ability of the provider, also use every kind of software including operating system (OS) and applications. Users were not responsible for controlling and managing the cloud infrastructure, they only have authority on OS, storage, distributed software and network components which were going to be used.

Platform as a service (PaaS): Users can develop and run software over cloud computing infrastructure via programming languages, libraries, services and with the tools that were supported by provider. Users were not responsible for controlling and managing network, server, OS and storage areas which were founded in cloud computing infrastructure, they can only interfere limited configuration changes. Software as a Service (SaaS): All the infrastructure, platform and software utilities were supported and provided by the provider. Users can privilege to service based applications via different devices and interfaces as thin clients and network browsers. There were only some limited configuration authorities over the service based applications that can be made by users.

3. CLOUD COMPUTING ATTACKS

As more companies move to cloud computing, look for hackers to follow. Some of the potential attack vectors criminals may attempt include:

A. Denial of Service (DoS) attacks

Some invulnerability professionals have argued that the cloud was more vulnerable to DoS attacks, because it was shared by many users, which makes DoS attacks much more damaging. When the Cloud Computing operating system notices the high workload on the flooded service, it will start to provide more computational power (more virtual machines, more service instances) to cope with the additional workload. Thus, the server hardware boundaries for maximum workload to process do no longer hold. In that sense, the Cloud system was trying to work against the attacker (by providing more computational power), but actually—to some extent—even supports the attacker by enabling him to do most possible damage on a service's availability, starting from a single flooding attack entry point. Thus, the attacker does not have to flood all n servers that provide a certain service in target, but merely can flood a single, Cloud-based address in order to perform a full loss of availability on the intended service [2]

B. Cloud malware injection attack

Attack attempt aims at injecting a unwanted service implementation or virtual machine into the Cloud system. Such kind of Cloud malware could serve any particular purpose the adversary was interested in, ranging from eavesdropping via subtle data modifications to full functionality changes. This attack creates its own mischievous service implementation module (SaaS or PaaS) or virtual machine instance (IaaS), and add it to the Cloud system. Then, the adversary has to trick the Cloud system so that it treats the new service instance as one of the valid instances for the particular service attacked by the adversary. If this succeeds, the Cloud automatically redirects user requests to the irrevelant service implementation, and the adversary's code was performed. A promising measure approach to this threat consists in the Cloud system performing a service instance integrity check prior to using a service instance for incoming requests. This can e.g. be done by storing a hash value on the original service instance's image file and comparing this value with the hash values of all new service instance images. Thus, an attacker would be required to guess that hash value comparison in order to inject his mischievous instances into the Cloud system. The idea of the Cloud Malware Injection attack was that an attacker uploads a manipulated copy of a victim's service instance so that some service requests service were processed within that mischievous instance. In order to achieve this, the attacker has to gain control over the victim's data in the cloud system (e.g. using one of the attacks described above). In terms of classification, this attack was the major representative of exploiting the service-to-cloud attack surface [3]. The attacker controlling the cloud exploits its privileged privilege capabilities to the service instances in order to attack that service instance's invulnerability domains.

C. Side channel attacks

An attacker try to understand the cloud by placing a mischievous virtual machine in close proximity to a target cloud server and then launching a side channel attack. Side-channel attacks have emerged as a kind of effective invulnerability threat targeting system implementation of cryptographic algorithms. Evaluating a cryptographic system's side-channel attacks was therefore important for secure system design [4].

D. Authentication attacks

Authentication was a weak in hosted and virtual services and was frequently targeted. There were many different ways to authenticate users; for example, based on what a person knows, has, or was. The functionality used to encrypt the authentication process and the methods used were a frequent target of attackers. Currently, regarding the architecture of SaaS, IaaS, and Paas, there was only IaaS this kind of information protection and data encryption. If the transmitted data was categorized to high confidential for any enterprise, the cloud computing service based on IaaS architecture will be the most suitable solution for secure data communication. In addition, the authorization of data process for those data belonged to the enterprises but stored on the service provider's side must be authorized by the user side to instead of the service providers. Most user-facing services today simple username and password type of knowledge-based authentication, with the exception of some financial which have deployed various forms of secondary authentication to make it a bit more difficult for popular attacks**.**

E. Man-In-The-Middle cryptographic attack

This attack was carried out when an attacker between two users. Anytime attackers can place themselves in the communication's path, there was the possibility that they can interrupt and modify communications.

4. AN ATTACK TAXONOMY FOR CLOUD COMPUTING

A cloud computing can be modeled using three different classes of participants: service users, service instances (or just services), and the cloud provider (Figure-2). Every interaction in a cloud computing can be addressed two entities of these participant. In the same way, every attack attempt in the cloud can be detailed into a set of interactions within this 3-class model. Hence, talking about cloud computing invulnerability means talking about attacks with the cloud provider among the list of participants [1]. This does not require the cloud provider to be mischievous; it may also just play an intermediate role in combined attack. Figure-2 was shown in Appendix.

a) Service-to-User
b) User-to-Service
c) Cloud-to-Service
d) Service-to-Cloud
e) Cloud-to-User
f) User-to-Cloud

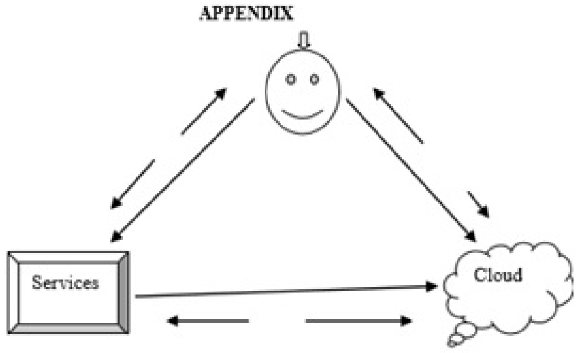

Figure-2. The computing cloud triangle and the six attack surfaces.

5. INVULNERABILITY IN CLOUD COMPUTING

While moving from traditional computing paradigm to cloud computing paradigm new invulnerability and privacy challenges has emerged. Invulnerability of the cloud computing system can be thought in two dimensions: physical invulnerability and cyber invulnerability. *Physical invulnerability* concerns the physical properties of the system. For example, a data Centre, which was owned by provider infrastructure, has to realize invulnerability standards and certifications globally, supervision and manageability on invulnerability prevention, uninterrupted power supplies, precautions for natural disasters (earthquake, flood, fire etc.) were critical [8]. However twenty four hours and seven days monitoring for heat, humidity and air condition systems and also some biometric entrance systems may help for the business continuity. On the other hand, *cyber invulnerability* defines the prevention of system from cyber world. There was a risk of cyber invulnerability attacks on services of cloud computing system. These attack can use huge amounts of computing resources, disables their usage by efficiently. In this section mostly known attack types were detailed. **Insider Attack:** Employee, entrepreneur and associates which were still or former attended who can or could privilege the whole information system with privileged authority were defined as *insider* [9]. Insider attacks were organized and knowledge about consumers or providers and include every kind of attacks which can be performed from inside [10, 11].**Flooding Attack:** In this type of attack, attackers can send very large amounts of packets from exploited information resources, and they were called as zombie [11]. Packets can be either of TCP, UDP, ICMP or a these protocols. These kinds of attacks were mostly realized over unauthorized network connections. Because of cloud computing paradigms' nature, connections to the virtual machines were established over Internet. For this reason, exposition of cloud users with *Denial of Service (DoS)* and *Distributed Denial of Service (DDoS)* attacks were inevitable. Flooding attacks affect the availability of serviced for authorized users. An attack that was realized to a server which serves one kind of service can prevent a vast of scale previligeibility to this served service. These kinds of attacks were called DoS attacks. If servers resources were after flooding attacks and it prevents the execution of other services, this kind of attacks were called indirect DoS attacks. **User to Root Attacks**: In this type of attack, an intruder grasps the account and password information of an authorized user, and Buffer overflows were used for establish console connection for authorized processes. This type of intrusion can be realized with writing an excessive amount of data to a statically defined buffers' capacity, and the information was captured by attackers An attacker who owned the account and password information of an authorized user can hold the privilege privilege to servers and also to virtual machines. **Port Scanning:** An attack that identifies open, closed and filtered ports on a system [8]. In port scanning, intruder scan seize information with the help of open ports like services that run on a system, IP and MAC addresses which belong to a connection, and router, gateway and firewall rules. TCP, UDP, SYN/FIN/ACK and Window scanning were the most common scanning attacks. Port scanning was not used by its own, an intruder realize the actual attack after getting information about open ports and running services.

Attacks on virtualization

After compromising hypervisor, control of the virtual machines in the virtual environment will be captured [10]. Zero day attacks were one of the methods that attack virtual machines and use hypervisor or other virtual machines to attack other virtual machines. Zero day attacks use known vulnerabilities before system or software developers apply patches or updates. Multiple virtual machines use the same resource pool, especially hardware and with this kind of privilege side channel data has a chance to be captured, which flow one virtual machine to other [9].

Backdoor Channel Attacks

A passive attack type in which attackers compromise a node in the cloud and use this compromised node as a zombie resource to execute a DDoS attack. Trojans and similar structures on the system were help to compromise the system. After compromising system become a zombie and also data can be approachable on the system [11].

Storage allocation and multi-tenancy

There were some issues to be defined about the data that were processed on cloud [6]. Owner and control of the data, maintaining audit records, how and how much of the audit records will be shared with the consumer. To ensure consumers' data privacy, provider has to realize isolation of data and guarantee in service level agreement.

Authorization, authentication, encryption, key and identity management

Different from conventional information technology, in cloud computing deployment of virtual machines, IP addresses and resources were dynamic [10]. Authorization, authentication and identity management have to be configured with affect less in the way of synchronization. While achieving this configuration, data privacy. And the way of achieving data privacy a well-defined, well configured and well-maintained key management.

Malicious insiders

In an IaaS, PaaS or SaaS environment that isn't built with the proper invulnerability, a mischievous insider can gain privilege to sensitive information such as a system administrator.

The CSA said that systems depend purely on the cloud service provider for in vulnerability were at great risk. The CSA also said that in its report "when encryption was performed, and if the keys were not kept with the consumer then the system was still vulnerable to mischievous insider attack".

Abuse of cloud services

Cloud computing has vast amounts of computing power, and allows organizations of all sizes to privilege the same, the CSA has warned that not everyone wants to use this power for good. For example, an attacker could use an array of cloud servers to crack an encryption key in minutes.

Cloud providers should consider how they can detect people abusing their service.

Lack due diligence

Some organizations were rushing to adopt cloud technologies without fully understanding the implications, according to the, Organizations need to perform extensive due diligence of their internal systems to fully understand the risks they're adopting with the new cloud model.

Shared technology vulnerabilities

The CSA said that the threat of shared vulnerabilities exists in all cloud delivery models. If a key piece of shared technology, such as the hypervisor was compromised, then it exposes the entire environments.

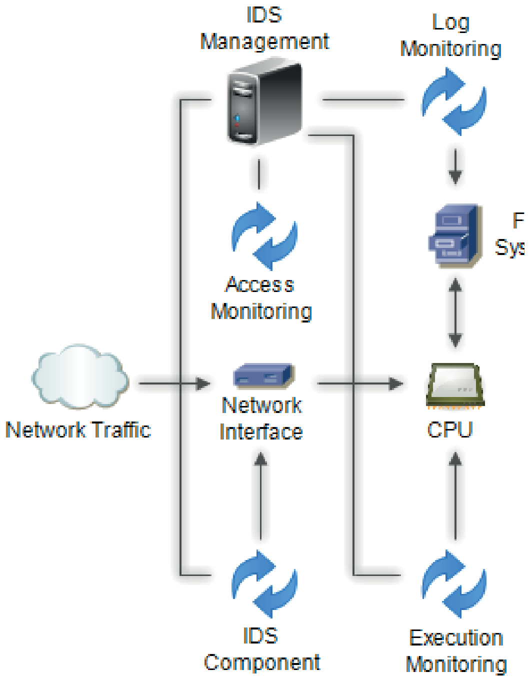

Figure-3. Host-based intrusion detection system architecture.

Data modification, forgery and integrity

Un trusted providers and system administrator can manipulate users' and consumers' data among to their own benefits [10]. Cloud users will be fall into a particularly bad position after such a manipulation or forgery occurs. This kind of integrity attacks can be prevented. Citations VM and some improvement were some solutions to prohibit tampering users' cloud data in the way of virtualization [10]

As cloud computing was on the rise, and especially due to its enormous attraction to organized criminals, we can expect to see a lot of invulnerability incidents and new kinds of vulnerabilities around it within the decades to come., thus making them more concrete and improving their analysis. Using the notion of attack surfaces, we deployed the developed classification taxonomy by means of four up-to-date attack incidents of cloud computing framework. Being a work-in-progress, we will continue with the collection and classification of cloud-based attacks and vulnerabilities in order to prove or refute our attack taxonomy's applicability and appropriateness.

Cloud computing vulnerabilities

Session riding: Session riding happens when an attacker steals a user's cookie to use the application in the name of the user. An attacker might also use CSRF attacks in order to trick the user into sending authenticated requests to arbitrary web sites to achieve various things.

Virtual machine escape: In virtualized environments, the physical servers run multiple virtual machines on top of hypervisors. An attacker can exploit a hypervisor remotely by using a vulnerability present in the hypervisor itself – such vulnerabilities were quite rare, but they do exist. Additionally, a virtual machine can escape from the virtualized sandbox environment and gain privilege to the hypervisor and consequentially all the virtual machines running on it.

Reliability and availability of service: We expect our cloud services and applications to always be available when we need them, which was one of the reasons for moving to the cloud. But this isn't always the case, The CSPs have uninterrupted power supplies, but even those can sometimes fail, so we can't rely on cloud services to be up and running 100% of the time. We have to take a little downtime into consideration, but that's the same when running our own private cloud.

Insecure cryptography: Cryptography algorithms usually require random number generators, which use unpredictable sources of information to generate actual random numbers, which was required to obtain a large entropy pool. If the random number generators were providing only a small entropy pool, the numbers can be brute forced movement and key presses, but servers were mostly running without user interaction, which consequentially means lower number of randomization sources. Therefore the virtual machines must rely on the sources they have available, which could result in easily guessable numbers that don't provide much entropy in cryptographic algorithms.

CSP Lock-in: We have to choose a cloud provider that will allow us to easily move to another provider when needed. We don't want to choose a CSP that will force us to use his own services, because sometimes we would like to use one CSP for one thing and the other CSP for something else.

Internet dependency: By using the cloud services, we're dependent upon the Internet connection, so if the Internet temporarily fails due to a lightning strike or ISP maintenance, the clients won't be able to connect to the cloud services. Therefore, the business will slowly lose money, because the users won't be able to use the service that's required for the business operation. Not to mention the services that need to be available 24/7, like applications in a hospital, where human lives were at stake.

User awareness: The users of the cloud services should be educated regarding different attacks, because the weakest link was often the user itself. There were multiple social engineering attack vectors that an attacker might use to lure the victim into visiting a mischievous web site, after which he can get privilege to the user's computer. From there, he can observe user actions and view the same data the user was viewing, not to mention that he can steal user's credentials to authenticate to the cloud service itself. Invulnerability awareness was an often overlooked invulnerability concern environment.

6. CONCLUSIONS

When an enterprise company wants to move their current operation to the cloud, they should be aware of the cloud threats in order for the move to be successful. We shouldn't rely on the cloud service provider to take care of invulnerability for us; rather than that, we should understand the invulnerability threats and communicate with our CSP to determine how they were addressing the invulnerability threats and continue from there. We should also create remote backups of our data regardless of whether the CSP was already providing backup service for us – it's better to have multiple data backups than figure out the data was not backed up at all when the need for data restoration arises.

REFERENCES

[1] Nils Gruschka. and Meiko Jensen. 2010. Attack Surfaces: A Taxonomy for Attacks on Cloud Computing. 3rd International Conference on Cloud Computing.

[2] Mohamed H. Sqalli, Fahd Al-Haidari. and Khaled Salah. 2011. EDoS-Shield- A Two- Steps Mitigation Technique against EDoS Attacks in Cloud Computing", 4th IEEE International Conference on Utility and Cloud Computing.

[3] M. Jensen, J. Schwenk, N. Gruschka. and L. Lo Iacono. 2009. On technical invulnerability issues in cloud computing. In: Proceedings of the IEEE International Conference on Cloud Computing (CLOUD-II).

[4] QiasiLuo. and Yunsi Fei. 2011. Algorithmic Collision Analysis for Evaluating Cryptographic System and Side-Channel Attacks. International Understanding The Cloud Computing StackSaaS, Paas, IaaS, © Diversity Limited, 2011 Non-commercial reuse with attribution permitted.

[5] G. Ateniese *et al*. 2007. Provable Data Possession at Untrusted Stores, Proc. ACM CCS‗07, October, pp. 598-609.

[6] Cong Wang, Qian Wang, Kui Ren. and Wenjing Lou. 2010. Privacy-Preserving Public Auditing for Data Storage Invulnerability in Cloud Computing‖ in IEEE INFOCOM 2010, San Diego, CA, March.

[9] Federal Information Processing Standards (FIPS) 140-2. (2001, May 25). Invulnerability Requirements for Cryptographic Modules. Gaithersburg, MD: National Institute of Standards and Technology (NIST). Retrieved from http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

[10] Voorsluys, William; Broberg, James; Buyya, Rajkumar (February 2011). "Introduction to Cloud Computing". In: R. Buyya, J. Broberg, A.Goscinski. CloudComputing: Principles and Paradigms. http://dwachira.hubpages.com/hub/Data-Invulnerability-Risks-In-Cloud-Computing.

[11] Abhishek Mohta, Ravi Kant Sahu. and LK Aisthi. Robust Data Invulnerability for Cloud while using Third Party Auditor, in International Journal of Advanced Research in Computer Science and Software Engineering. Vol. No. 2, I.