RESEARCH ARTICLE OPEN ACCESS

Key Architectural Models, Security Issues and Solutions on Cloud Computing

Andemariam Mebrahtu [1], Balu Srinivasulu [2]
Department of Computer Science
Eritrea Institute of Technology
Asmara –Eritrea

ABSTRACT
Cloud computing is a recent advancement wherein IT infrastructure and applications are provided as "services" to end-users under a usage-based payment model. Many organizations, such as Google, Amazon, IBM and many others, accelerate their paces in developing Cloud computing systems and providing services to user with best affords but there phases many difficulties regarding security problem and users also afraid toward security of own data i.e. whether cloud providers able to maintain data integrity ,confidentiality as well as authentication. To resolve the security issues in cloud computing, this paper presents various solutions for different issues.

Keywords:- Cloud Computing, Cloud Security, IaaS, file allocation table (FAT), Hypervisor.

I. INTRODUCTION

Cloud computing provides its user with many capabilities like accessing a large number of applications without the need for having a license, purchasing, installing or downloading any of these applications. It also reduces both running and installation costs of computers and software as there is no need to have any infrastructure. Users can access information anywhere, all they need is to connect to a network (usually the Internet).
Cloud computing offers companies an increased storage than traditional storage systems. Software updates and batches are highly automated with reduced number of hired highly skilled IT personnel. [1], [2]. Cloud computing can be divided according to deployment models and according to service delivery models which can be found in the following subsections.

A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services), that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three delivery models, and four deployment models [3].

Major advantages of cloud computing are low costs and high convenience. Since cloud computing is accessible and centralized, therefore, new opportunities are created for security breaches. Cloud computing security can be estimated through both the offensive and defensive perspectives. In this paper classification of various attacks and models in cloud to examine to what degree proposed defenses can address are going to be discussed.

Characteristics of cloud computing

As outlined by Mel and Grance [4], cloud computing generally has five characteristics. They are shown in the following diagram as follows

- On Demand Self Service: Cloud Computing allows the users to use web services and resources on demand. One can logon to a website at any time and use them.

- Broad Network Access: Since cloud computing is completely web based, it can be accessed from anywhere and at any time.

- Resource Pooling: Cloud computing allows multiple tenants to share a pool of resources. One can share single physical instance of hardware, database and basic infrastructure.

- Rapid Elasticity: It is very easy to scale the resources vertically or horizontally at any time. Scaling of resources means the ability of resources to deal with increasing or decreasing demand. The resources being used by customers at any given point of time are automatically monitored.

- Measured Service: In Measured service cloud provider controls and monitors all the aspects of cloud service. Resource optimization, billing, and capacity planning etc. depend on it.

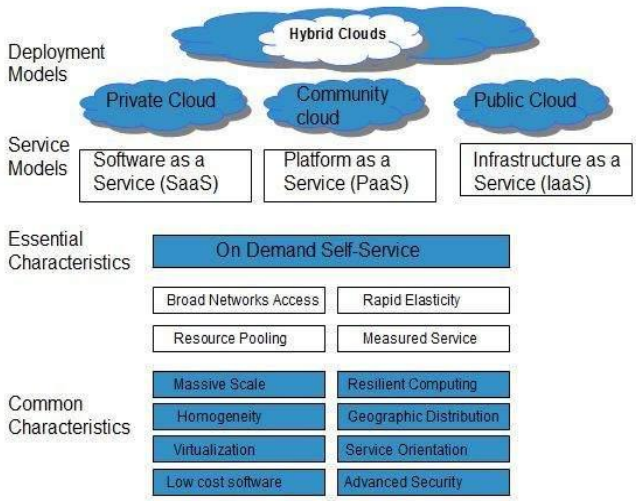

Fig1. Cloud computing characteristics and architecture

II. CLOUD COMPUTING INFRASTRUCTURE

Even based on the brief overview given so far, we can see some potential security pitfalls looming: sharing resources that are not in one's control with others is always likely to be a venture fraught with risks. In this section we look at the infrastructure that implements the concepts detailed previously in order to better grasp the intricacies of the possible security problems we might face.

A. Cloud service models

The amount of resources exposed over a network can depend on the type of service that a vendor is providing to its customers. Different services give rise to different security concerns, and may even lead to different parties being responsible for handling said concerns. [1]

Cloud computing providers offer three fundamental service models: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS):

- Infrastructure as a Service (IaaS)

In this model, the vendor provides physical computer hardware, including data storage, CPU processing and network connectivity. The vendors may share their hardware among Cloud Service Customers (CSC) by using virtualization software. IaaS allows customers to run control and maintain operating systems and software applications of their choice, but the vendor typically controls and maintains the physical computer hardware. This leads to the customer being more responsible for handling their own data security with the vendor being more responsible for physical security, since they own and manage the physical devices being used as infrastructure. Examples of IaaS vendor services include Go Grid, Amazon Elastic Compute Cloud (EC2) and Rackspace Cloud.

- Platform as a Service (PaaS)

In this model, the vendor provides not only Infrastructure as a Service, but also the operating systems and server applications that their customers use. PaaS lets customers use the vendor's cloud infrastructure to deploy user made web applications/software. Typically the vendor controls and maintains the physical computer hardware, operating systems and server applications while the customer only controls and maintains their developed software applications. Customers would therefore be mainly responsible for any security exploits that could target their applications, while the vendor is not only responsible for physical security, but also for any security exploits that could target network connections, data storage and data access. Examples of PaaS vendor services include Google App Engine, Force.com, Amazon Web Services Elastic Beanstalk, and the Microsoft Windows Azure platform.

- Software as a Service (SaaS)

In this model, the vendor provides customers with software applications using their cloud infrastructure and cloud platforms. These end user applications are typically accessed by users via web browser, as such there is no need to install or maintain additional software. The vendor typically controls and maintains the physical computer hardware, operating systems and software applications while the customer only controls and maintains certain application configuration settings specific to them. The vendor is mainly responsible for ensuring all forms of security in this service. Examples of SaaS vendor services include Google Docs, Google Gmail and Microsoft Office 365.From this subsection, it is fairly clear by now that the level of responsibility shared between CSPs and CSPs differs based on the service model being employed.

B. Cloud deployment models

There are four types of cloud computing deployment models:

- Public Clouds**:** A public cloud is a publicly accessible cloud environment owned by a third-party cloud provider. The IT resources on public clouds are usually provisioned via the previously described cloud delivery models and are generally offered to cloud

consumers at a cost or are commercialized via other avenues (such as advertisement). The cloud provider is responsible for the creation and on-going maintenance of the public cloud and its IT resources. Many of the scenarios and architectures explored involve public clouds and the relationship between the providers and consumers of IT resources via public clouds.

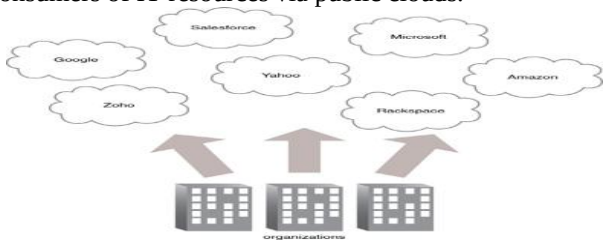

Fig2. Show partial view of the public cloud landscape, highlighting some of the primary vendors in the marketplace.

➢ Community Clouds: A community cloud is similar to a public cloud except that its access is limited to a specific community of cloud consumers. The community cloud may be jointly owned by the community members or by a third-party cloud provider that provisions a public cloud with limited access. The member cloud consumers of the community typically share the responsibility for defining and evolving the community cloud (Fig2). Membership in the community does not necessarily guarantee access to or control of all the cloud's IT resources. Parties outside the community are generally not granted access unless allowed by the community.

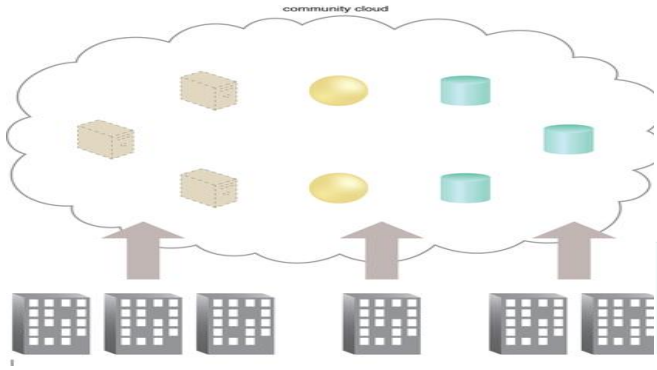

Fig3. An example of community cloud accessing IT resources from a community cloud.

➢ Private Clouds: A private cloud is owned by a single organization. Private clouds enable an organization to use cloud computing technology as a means of centralizing access to IT resources by different parts, locations, or departments of the organization. When a private cloud exists as a controlled environment, the problems described in the Risks and Challenges section do not tend to apply. The use of a private cloud can change how organizational and trust boundaries are defined and applied. The actual administration of a private cloud environment may be carried out by internal or outsourced staff.

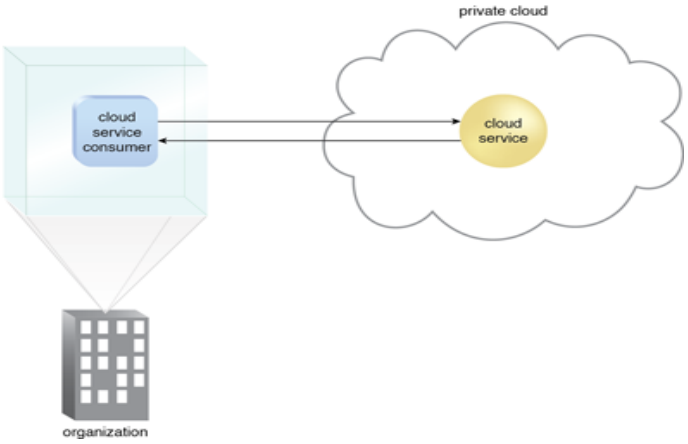

Fig4. A cloud service consumer in the organization's on-premise environment accesses a cloud service hosted on the same organization's private cloud via a virtual private network.

➢ Hybrid Clouds: A hybrid cloud is a cloud environment comprised of two or more different cloud deployment models. For example, a cloud consumer may choose to deploy cloud services processing sensitive data to a private cloud and other, less sensitive cloud services to a public cloud. The result of this combination is a hybrid deployment model (Fig5).

Fig5. An organization using a hybrid cloud architecture that utilizes both a private and public cloud.

Hybrid deployment architectures can be complex and challenging to create and maintain due to the potential disparity in cloud environments and the fact that management responsibilities are typically split between the private cloud provider organization and the public cloud provider.

III. CLOUD SECURITY ATTACKS

The evolution of cloud computing is from many different technologies such as virtualization, grid computing, autonomic-computing, and some other technologies. New challenges arise whenever a new technology comes. In general, cloud computer security identifies following main objectives [5]:

1. Availability: The goal of availability for Cloud Computing systems is to ensure that data and services are always available for its users at any time, at any place.
2. Confidentiality: The goal of confidentiality is to keep users data secret in the Cloud systems by making it available only to eligible entities and no unauthorized access to data can be obtained.
3. Integrity: The goal of Data integrity in the Cloud system is to assure that data has not been altered in any way while it is stored or while its transport over the network.
4. Authentication: The goal of authentication is to assure the identity of the entity involved in the communication.
5. Accountability: The goal of accountability is to assure that no entity can deny its participation in a data transfer between them.

These security objectives require the employment of certain security mechanisms and services to be implemented. A security mechanism can be defined as a process, or a device, which aimed to detect, or prevent, or recover from a security attack. Security mechanisms like stenography, encryption, hashing etc. are commonly used in providing security to a system. A Security Service can be identified as a processing or communication service aimed to enhances the security of data and the information transfers of an entity. These services help in countering security attacks. Security services usually employ one or more security mechanism to achieve its goals. As the world is moving towards cloud computing, it become more sophisticated and attackers look to follow it. Some of the potential attacks on cloud computing are:

A. Denial of Service (DoS) attacks

In DoS attack, an attacker overloads the target cloud system with service requests so that it stops responding to any new requests and hence made resources unavailable to its users. Some Cloud Security Alliance has identified that the cloud is more vulnerable to DoS attacks, because it is used by so many users which makes it much more damaging.DOS attacks are [5]

1. An attacker can overload the target with large amount of junk data that consume the network bandwidth and resources, for example UDP floods, ICMP floods etc.
2. An attacker can make use of blank space (lacuna) that associated with various networking protocol to overload target resource, for example SYN floods, fragment packet attack, ping of death etc.
3. An attacker can make HTTP request in large amount so that it cannot be handled by the server for example HTTP DDOS attack, XML DDOS attack etc.

Possible solutions against DoS attacks

For restricting DoS attack we can classify traffic on the basis of authorization, owe can block traffic that are identify as unauthorized and allow traffic that are identify as authorized. For this firewalls can be used to allow or deny traffic on the basis of access protocols, ports or IP addresses. Today most of the switches have capability of rate-limiting on the basis of Access Control List that can provide automatic rate limiting, shape traffic, bogus IP filtering, binding and can deeply inspect packets. Similar to switches routers have also some capability like ACL and rate-limiting which can be set manually to create rules and regulations.

Application front end hardware can be used on networks in colligation with routers and switches which can analyze data packets as they enter into the network system to check their authority and priority so that flow of traffic can be controlled. After DoS attack one can send all the traffic on attacked packet to a null interface or to a non existing interface, this helps to reduce the effect of DoS attack.

B. Cloud Malware Injection Attack

In Cloud Malware Injection Attack an attacker tries to inject malicious service or virtual machine into the cloud. In this type of attack attacker creates its own malicious service implementation module (SaaS or PaaS) or virtual machine instance (IaaS), and try to add it to the Cloud system. Then, the attacker has to behave so as to make it a valid service to the Cloud system that it is some new service implementation instance among the valid instances. If the attacker succeeds in this, the Cloud automatically redirects the requests of valid user to the malicious service implementation, and the attacker code starts to execute. The main scenario behind the Cloud Malware Injection attack is that an

attacker transfers a malicious service instance into cloud so that It can achieve access to the service requests of the victim's service [6].
To achieve this, the attacker has to derive control over the victim's data in the cloud. According to classification, this attack is the major representative of exploiting the service-to-cloud attack surface. The purpose of cloud malware injection attack can be anything in which an attacker is interested; it may include data modifications, full functionality changes/reverse or blockings.

Possible solutions against malware injection attacks

In cloud computing system application run by the customer are considered with high efficiency and integrity. So to prevent cloud from malware injection attack we can combine the integrity with hardware or can use hardware for integrity purpose because for an attacker it is difficult to intrude in the IaaS level. For this we can utilize a file allocation table (FAT) system, by using it we can determine the validity and integrity of new instance by comparing the current and previous instance. For this purpose, we need to deploy a hypervisor on the provider's side. In cloud system hypervisor is considered to be the most secure and sophisticated part of it whose security cannot be broken by any means.
The Hypervisor is responsible for scheduling all the instance and services so we can make hypervisor to check file allocation table to validate and integrate an instance of customer. Other approach is that we can maintain the information of the platform type version that a customer user to access the cloud in first phase when a customer open an account and can use those information to check the validity of new instance of the customer.

C. Side Channel Attacks

An attacker attempts to compromise the cloud system by placing a malicious virtual machine in close proximity to a target cloud server system and then Launching a side channel attack. Side-channel attacks have emerged as a kind of effective security threat targeting system implementation of cryptographic algorithms. Evaluating cryptographic systems resilience to side-channel attacks is therefore important for secure system design. Side channel attacks use two steps to attack-VM CO-Residence and Placement i.e.an attacker can often place his or her instance on the same physical machine as a target instance and VM Extraction i.e., the ability of a malicious instance to utilize side channels to learn information about co-resident instances. It can be very easy to gain secret information from a device so security against side channel attack in cloud computing should be provided [7].

Possible solutions against Side Channel attacks

To prevent cloud from side channel attack we can use combination of virtual firewall appliance. According to the case study of Amazon EC2 service it is possible for an attacker to instantiate new virtual machine to identified targeted virtual machine in cloud and extracts some confidential information. But a virtual firewall prevents this attempt of placement of malicious virtual machine during a side channel attack.
Another approach is to use randomly encryption decryption (using concept of confusion diffusion) because it prevent second step extraction of side channel attack. Here by confusion we mean that making relation between plain and cipher text more and more complex; by diffusion we mean to dissipate the statistical structure of plaintext over the bulk of cipher text. Security against both front end and back end side of cloud computing architecture is provided by this combination and also provide RAS (Reliability, Availability, and Security).
When we use randomly encryption decryption we mean that customer data or information encrypted through different encryption algorithm so attacker faces more difficulties to detect or extract cryptography key.

D. Authentication Attacks

Authentication is a weak point in cloud computing services which is frequently targeted by an attacker. Today most of the services still use simple username and password type of knowledge-based authentication, but some exception are financial institutions which are using various forms of secondary authentication (such as shared secret questions, site keys, virtual keyboards, etc.) That makes it more difficult for popular phishing attacks. Some authentication attacks are [8] [9]:

1. Brute Force Attacks: In this type of attack, all possible combinations of password apply to break the password. The brute force attack is generally applied to crack the encrypted passwords where the passwords are saved in the form of encrypted text.
2. Dictionary Attack: This type of Attack is relatively faster than brute force attack . Unlike checking all possibilities using brute force attack, the dictionary attack tries to match the password with most occurring words or words of daily life usage.
3. Shoulder Surfing: Shoulder Surfing is an alternative name of "spying" in which the attacker spies the user's movements to get his/her password. In this type of attack the attacker observes the user; how he enters the password i.e. what keys of keyboard the user has pressed
4. Replay Attacks: The replay attacks are also known as the reflection attacks. It is a way to attack challenge response user authentication mechanism.

5. Phishing Attacks: It is a web based attack in which the attacker redirects the user to the fake website to get passwords / Pin Codes of the user.
6. Key Loggers**:** The key loggers are the software programs which monitors the user activities by recording each and every key pressed by the user.

Possible solutions against Authentication attacks

Delayed response: Given a login-name/password pair the server provides a slightly delayed yes/no answer (say not faster than one answer per second). This should prevent an attacker from checking sufficiently many passwords in a reasonable time.
1. Account locking: Accounts are locked after a few unsuccessful login attempts (for example, an account is locked for an hour after five unsuccessful attempts.) Like the previous measure, this measure is designed to prevent attackers from checking sufficiently many passwords in a reasonable time.
2. Biometrics: Biometric is an image-based authentication system in which finger prints, face, iris, retinal, speech, signature verification are used to verify against the original specimen. The image is preprocessed first and then the classification of images is done. The advantage of this method is that it is real and unique signature and cannot be stolen. The disadvantage is that it is costly and difficult to implement. It is not a completely matured method and it can be easily compromised and is time consuming also.

E. Man-In-The-Middle Cryptographic Attacks

A man in the middle attack is one in which the attacker intercepts messages in a public key exchange and then retransmits them, substituting his own public key for the requested one, so that the two original parties still appear to be communicating with each other. In the process, the two original parties appear to communicate normally. The message sender does not recognize that the receiver is an unknown attacker trying to access or modify the message before retransmitting to the receiver. Thus, the attacker controls the entire communication. Some type of MIM attacks are [10]:
1. Address Resolution Protocol Communication (ARP): In the normal ARP communication, the host PC will send a packet which has the source and destination IP address inside the packet and will broadcast it to all the devices connected to the network. The device which has the target IP address will only send the ARP reply with its MAC address in it and then communication takes place. The ARP protocol is not a secured protocol and the ARP cache doesn't have a foolproof mechanism which results in a big problem.
2. ARP Cache Poisoning: In ARP cache poisoning, the attacker would be sniffing onto the network by controlling the network switch to monitor the network traffic and spoof the ARP packets between the host and the destination PC and perform the MIM attack.
3. DNS Spoofing: The target, in this case, will be provided with fake information which would lead to loss of credentials. As explained earlier this is a kind of online MIM attack where the attacker has created a fake website of your bank, so when you visit your bank website you will be redirected to the website created by the attacker and then the attacker will gain all your credentials.
4. Session Hijacking: In this once the session is established between the host PC and the web server the attacker can obtain certain parts of the session establishment which is done by capturing the cookies that were used for the session establishment.

Possible solutions against Authentication attacks:
1. By using one time password because one time password is immune to MIM attacks.
2. By forensic analysis of MIM attacks
   - IP address of the server
   - Is the certificate self signed?
   - Do other clients, elsewhere on the Internet, also get the same certificate?
   - Is the certificate signed by a trusted CA?
3. By using mutual authentication, with many client and server implementations, the initial trust is only confirmed by one way verification between the client and the server. With mutual authentication, the server verifies the client and the client verifies the server to ensure legitimate communications are being exchanged.
4. Verification can be conducted by using public and private keys.

IV. CONCLUSIONS AND FUTURE WORK

Cloud computing is revolutionizing how information technology resources and services are used and managed, but the revolution always comes with new problems. We have depicted some crucial and well known security attacks and have proposed some potential solutions in this paper, such as utilizing the FAT table and a Hypervisor.

In the future, we will extend our research by providing implementations and producing results to justify our concepts of security for cloud computing. The concepts we have discussed here will help to build a strong architecture for security in the field of cloud computation. This kind of structured security will also be able to improve

customer satisfaction to a great extent and will attract more investors in this cloud computation concept for industrial as well as future research farms. Lastly, we propose to build strong theoretical concepts for security in order to build a more generalized architecture to prevent different kinds of attacks.

REFERENCES

[1]. Nidal M. Turab ,Anas Abu Taleb ,Shadi R. Masadeh, "Cloud Computing Challenges And Solutions" International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.5, September 2013

[2]. Cloud security alliance "Security guidance for critical areas of focus in cloud computing V3.0" https://cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-focus-in-cloud-computing.

[3]. P. Mell and T. Grance, "The nist definition of cloud computing (draft)," NIST special publication , vol. 800, no. 145, p. 7, 2011.

[4]. T. Grance and P. Mell, "The nist definition of cloud computing," National Institute of Standards and Technology (NIST), 2011.

[5]. Priyanka Chouhan, Rajendra Singh," Security Attacks on Cloud Computing With Possible Solution", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 1, January 2016,ISSN: 2277 128X

[6]. Shikha Singh , Binay Kumar Pandey , Ratnesh Srivastava , Neharawat ,Poonamrawat , Awantika "Cloud Computing Attacks: A Discussion With Solutions", Open Journal Of Mobile Computing And Cloud Computing, Volume 1, Number 1, August 2014.

[7]. B. Sevak, "Security against side channel attack in cloud computing," International Journal of Engineering and Advanced Technology (IJEAT), vol. 2, no. 2, p. 183, 2013.

[8]. Kim, J. and Hong, S. (2012). A Consolidated Authentication Model in Cloud Computing Environments. International Journal of Multimedia and Ubiquitous Engineering, 7(3), 151-160.

[9]. Han, J., Susilo, W. and Mu, Y. (2013). Identity-based data storage in cloud computing. Future Generation Computer Systems, 29, 673–681. doi:10.1016/j.future.2012.07.010

[10]. K. Haataja and P. Toivanen. Practical Man-in-the-Middle Attacks Against Bluetooth Secure Simple Pairing. In 4th International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM'08, pages 1–5, Oct. 2008.

[11]. Catteddu, D.: Cloud Computing: benefits, risks and recommendations for information security. Springer, 2010

[12]. Perez-Botero, D., Szefer, J., Lee, R.B.: Characterizing hypervisor vulnerabilities in cloud computing servers. In: Proceedings of the 2013 international workshop on Security in cloud computing, pp. 3–10. ACM, 2013

AUTHORS

Mr. Andemariam Mebrahtu, Currently I am working as Lecturer and HOD in *Department of Computer Science, Eritrea Institute of Technology, Asmara, Eritrea.* I have sound experience in teaching and academic administration activities. My area of interest includes Cloud Computing, Distributed Computing and Big Data Management.

Mr. Balu Srinivasulu currently I am working as a Lecturer in the *Department of Computer Science, Eritrea Institute of Technology, Asmara, Eritrea.* I have wide experience of teaching and research in field of Computer Science. I have published a number of international journal papers related to the Computer Science. My areas of research are Wireless Network, Communication Networks and Cloud Computing.