SECURITY AND PRIVARTY IN THE CLOUD COMPUTING

[1]Muaz Gultekin *[2]Halil İbrahim Şanlan [3]Mehmet Yilmaz
*[1]Faculty of Engineering, Department of Computer Engineering Yalova University, Turkey

Abstract

Cloud computing if one of the most important technologies for web services models and web data storage that cause an acceleration in use of the cloud environment services. But this bring some security issues together .In the cloud service environment when a third party, if the data and business applications, providing privacy and security issues as outsourcing has become a major concern. By the way cloud environments are available in a common goal to provide a comprehensive review of existing security and privacy issues. These targets were identified as a security and privacy attributes which is represented as confidentiality, integrity, availability, accountability and privacy-maintainability. In this study we have suggested a novel approach which based on scenario defense strategies. Thanks to this solution cloud computing can prevent threats more easily.

Key words: Cloud computing, confidentiality, integrity, availability, accountability, represented and privacy-maintainability

1. Introduction

"Cloud computing; a large scale in the pool (so isolated, virtual, dynamic which can be measured, managed information processing power, storage) as on-demand computing is a paradigm that provides services over the internet." ((The European Network and Information Security Agency (ENISA))

"Cloud computing can be configured in the public pool of processing resources everywhere, available on demand, is a model that provides network access." ((The US National Institute of Standards and Technology (NIST)). NIST definition of cloud repositories lists five basic characteristics; on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service or expansion. It also includes three basic service model. In these three services Software as a service (SaaS), Platform as a service (PaaS) and Infrastructure as a service (IaaS).

The rapid development of current information technology, electronic publishing is becoming more and more popular as a digital photo and video distribution. Digital multimedia content such as photos and videos can be easily sent over the Internet to the cloud system. Cloud computing cloud service providers to host their data or has become an important technology to perform computing tasks.

Virtualization, cloud computing is the name of one of the concepts that we most recently heard me. We can develop lot of definitions for virtualization. But the most basic definition of the article in order to extend the course; "Physically, hardware components, multiple operating

*Corresponding author: Address: Faculty of Engineering, Department of Computer Engineering Yalova University, Turkey

systems can be installed using software technologies." As we can. Our structure through virtualization becomes more flexible and efficient. Virtualization is one of the key technologies used in the IaaS (Infrastructure as a service) cloud infrastructure. For example, virtualization, used in the delivery of cloud services by major cloud service providers such as Amazon and Microsoft

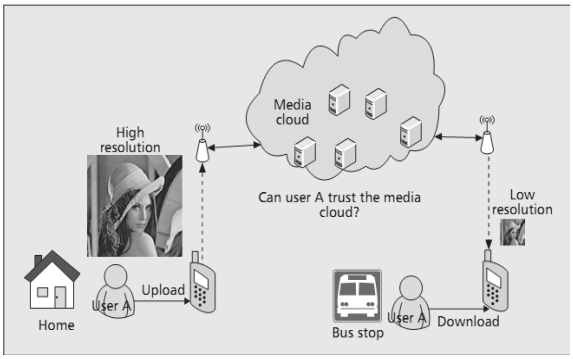

Fig 1. Can user A trust the media cloud?

As shown in Figure 1, the user is at home by using A cell phone that user installs the media cloud image. Then at the bus stop when the media from the cloud wants to access the same environment (such as an image). User A is media data has not been modified by others should be guarantee that.

Reasonable cloud system can provide security access control. However, it may not be reliable cloud is managed by a third party, such as our own, even cloud service providers. Security can only be guaranteed by contracts between the users and cloud service providers. These include some potential risks, security attacks and cloud administrator's duties, such as abuse.

Cloud services to a point where the top from the bottom layer can be presented in a variety of ways. Typically, modern data centers are supported by. Cloud stack, each layer of a service model represents. Infrastructure (IaaS) service sources are collected and managed physically delivers it in the substrate. Services storage (e.g., googlefs) is delivered in forms. Network (for example, Openflow) or computational ability (eg, Hadoop MapReduce). Middleware Platform Service (SaaS); provide services as a programming environment (eg. Django). Software is run (Google App Engine). An area where service at the top layer (SaaS) offering software for cloud providers to serve as a software application that provides flexibility to the client.

2. SECURITY AND PRIVACY CHALLENGES

Different safety in every domain in the cloud computing environment, privacy, can use a variety of mechanisms and requirements in confidence and potential employment multiple interfaces and semantic domain is required. Individually enabled services such domains or may represent other infrastructure components or applications. Now let us examine the affected components.

2.1. Authentication and Identity Management

Authentication, users who request an application or system is to check whether it exists in the system. A system without authorization (Authorization) primarily for user authentication (Authentication) must make. After making system interfaces allow the user to provide Authentication of the system and the user decides whether the user is authorized where. Different authentication tokens and use of identity negotiation protocols which can cause undesirable situation. Password-based authentication has an inherent limitation of current and pose a significant risk. An IDM system must protect private and sensitive information for users and processes. That multi-tenant cloud environments, how it affects privacy Dunn credentials are not yet well understood. Multi-tenant environment, providers must allocate customer identity authentication information. Identity and the IDM components should be easily integrated with other security components.

2.2. Access Control and Accounting

Access control services in catching dynamic content and nature or identity-based access requirements should be flexible enough to apply the principle of least privilege. Manageability and distribution of privileged access to systems used in the clouds is important to provide an efficient application. The access control model should capture aspects of SLA(Service Level Agreement).
An important issue in the accounting records could be the customer does not want to have a way out detailed information. Outsourcing and multi-tenant cloud the work done is accelerate the fear of customers. Therefore privacy is very important and cloud providers to wriş control and accounting services is obliged to provide confidence in this regard.
Access control services in catching dynamic content and nature or identity-based access requirements should be flexible enough to apply the principle of least privilege. Manageability and distribution of privileged access to systems used in the clouds is important to provide an efficient application. The access control model should capture aspects of SLA(Service Level Agreement).
An important issue in the accounting records could be the customer does not want to have a way out detailed information. Outsourcing and multi-tenant cloud the work done is accelerate the fear of customers. Therefore privacy is very important and cloud providers to wriş control and accounting services is obliged to provide confidence in this regard.

2.3. Trust Management and Policy Integration

Although multiple service providers offer different services to different clouds and despite their different approach to security arising from them should work to provide a heterogeneous environment. Cloud service providers need to create multiple services to develop great applications services. To monitor the safety and security breaches that are required for a dynamic cooperation is needed for such an integrated mechanism. Security breaches in the compliance stage of this integration can be the median. Therefore, they must demonstrate the integration process in order to make the control mechanisms that control the emergence of any security breach. Heterogeneity, interoperability, and secure cloud management policy integration policy

evaluation must take their duties. It is also very important to communicate positively with customers passed.

2.4. Secure-Service Management

Cloud computing environments in the cloud service providers and service integrators to provide services to the customer service they give. Independent service providers are providing the service integrator with consistent and organized in a way to ensure the protection needs of the customers as well as work. Many cloud service providers, despite using Web Services Description Language (WSDL), does not fully meet their cloud computing services. Clouds, so the price of such a service and the quality of service issues such as SLA (Service Level Agreement) search and composition are important. These issues should be addressed to define services, the best workable options to integrate all operations should be the policy of the service provider must ensure realization of customer satisfaction.

2.5. Privacy and Data Protection

We consider privacy to date, including the need to protect credentials during the integration policy components and transaction history are the very core of the subject. Many organizations maintain data instead of hosting their own site is outside somewhere. This cloud is the single biggest fear of the customers. This data may contain private information of the customer data they share and become at risk by installing outside. Cloud service providers must provide customers with a high level of transparency on this issue and provide. Privacy protection mechanisms should be embedded in all security solutions. Cloud computing is available trace back, such as audit and tairh-based access control for a variety of purposes.

User's network traffic and data must be protected against unauthorized access. Users can load data using a SaaS(Software as a Service) cloud, you need to prevent users who are not authorized to read the data stored in the cloud. A PaaS (Platform as a Service) provider offers a development environment to build Web services or applications and so have similar privacy concerns. As IaaS (Infrastructure as a Service), multiple users can rent a single physical infrastructure computing resources. A user should be able to view another user's memory usage status or source.

2.6. Organizational Security Management

Existing security management and information security lifecycle of business modeling with the acceptance of cloud computing has led to major changes. Despite the potential benefits of using cloud may lead to coordination between the different communities of interest within client organizations. Cloud providers are required to act according to her natural disasters calculate all the factors, such as economic risks. Threats arising from the inside should be considered. Cherry in a multi-tenant environment may be highly targeted attack victim, after dukes users should know how to be affected by this attack. Risk assessment in this field should be consistent and realistic measurements.

2.7. Integrity

Varies depending on the model and services mentioned herein integrity so aggressive attacks usually focus on different targets such as network traffic or virtual disks.

2.8. Availability

Availability of services is required to continue to provide services or the server. If you are not a positive thing for this service does not meet the service drop to the attack. Domain Name System (DNS) attacks are usually used in the attack. DNS attacks are not new in the IT security field. However, the attacks are still problematic due to the characteristics of cloud computing wide network access.

2.9. Cloud Characteristics and Security Challenges

Cloud Security summarized five basic characteristics of traditional computing paradigm showing differences.

2.9.1. Outsourcing

Individuals and businesses need to store more data and use it to do more. (Ee-mail, photo albums, tax documents, financial transactions vb.) Cloud environment can promote in terms of cost-effectiveness and their own privacy and data integrity may be at risk. Can encrypt your data to prevent data access by unwanted users. Encryption is also made use of the traditional data service delivery. Is a difficult task plain text search or query on the database?

Another important issue, the external data source data integrity is maintained by cloud service providers. Clouds may be tempted to be economic, but data integrity and availability does not guarantee. This problem may prevent the successful deployment of a cloud architecture if not taken properly. Traditional encryption techniques to verify the users' local data will not be enough. You need a local copy of the data to verify the data integrity, the data is sourced to determine which external.

2.9.2. Multi-tenancy

Multi-tenancy means that the cloud platform is shared and utilized by multiple customers. Multi-tenancy means that the cloud platform is shared and utilized by multiple customers

2.9.3. Massive data and intense computation

Cloud computing is capable of handling mass data storage and intense computing tasks. Therefore, traditional security mechanisms are not sufficient due to the unbearable burden of computation or communication. For example, to remotely verify the integrity of stored data, this is not practical.

3. CLOUD THREATS

Data center network (DCN), virtualization, distributed storage, MapReduce, web applications and services is a collection of existing techniques such as. Modern data center has been employed as an effective carrier of practical cloud environments. This large computation and storage capability allows the output of the machine with the techniques of DCN. Provide resource allocation and serves as the virtualization technology. Cooperation can be found with Virtualization, multiple connections are installed on the same physical machine and nothing blocking. MapReduce is a programming framework that supports distributed computing and data sets.

3.1. Cloud Vulnerabilities

3.1.1. VM co-residence

Multiple independent customers on the same physical infrastructure, the means to share concretely, the virtual machine is placed on the different clients on the same physical machine.

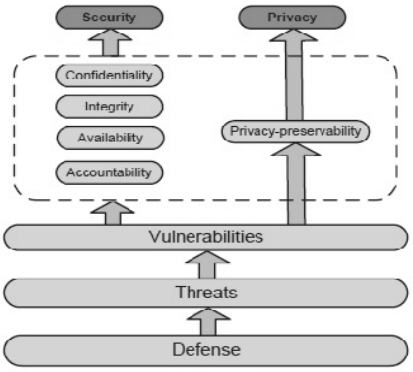

Fig. 2. Ecosystem of Cloud Security and Privacy

3.1.2. Loss of Physical Control

Data and programs of the cloud customer is outsourced to the cloud server, cloud of data sets and programs directly lose control. Some of the attacks and the physical loss of control clients can resist accidents. For example, the data or software has changed, lost, or even, in addition to this can be deleted. Traditional methods of data / calculation to ensure the integrity and privacy is difficult and is not practical.

3.1.3. Cloud Pricing Model

Cloud server time, bandwidth, and storage, in terms of measurements such as determining the cost of services on a pay-as-you-go pricing model is presented. All Customers use cloud services responsible for financially. Attackers pricing model by exploiting the billing process incentives for abuse. For example EDos(Distributed Denial of Service Attack) attacks cloud manages a new pricing model for clients and causes costs inextricable.

3.2. Threats to Cloud Confidentiality

3.2.1. Cross-VM attack via Side Channels

3.2.1.1. Step 1: placement

An adversary needs to place a malicious VM on the physical server where the target client's VM is located. The purpose is to take place at the client VM. To achieve this, the first target of the instance of the VM to determine the location... This network is nmap, Hping, tools such as wget, etc can be done. An enemy, it is possible to determine whether two VM instances. 1) Comparing Domain0's IP addresses to see if they match, and 2) measuring the small packet round-trip time can do this check.

3.2.1.1. Step 2: extraction

A malicious VM has co-resided with the victim VM. Malicious VM and victims, physical resources, data, cache, network access, the CPU branch predictors, the CPU pipelines, such as sharing is a way of enemy attacks. Server load current predictable and can measure the use of the cache.

- The number of visitors or you can obtain the desired pages more often
- To steal a victim's password measures the time between keystrokes.

3.3. Threats to Cloud Availability

3.3.1. Flooding Attack via Bandwidth Starvation

Torrent assault is sent a large amount of meaningless requests. The purpose is to prevent the proper operation of the service. Direct DOS attacks target is determined and the cloud service availability enables the losing completely.

- Target victims that are hosted in the same physical machine, all services are affected.

Cloud providers a service level Agreement with its clients (SLA) must be signe because customers will be aware of the corruption that. A DOS attack (bandwidth starvation), there are several steps to start effectively:

- Topology identification

If multiple routers share abuse, the number of routers between two computers can be determined.

- Gaining access to enough hosts sufficient host access for users.
- carrying out the attack.

 Fake resource consumption (FRC) attacks.

Attackers' legal acts as a cloud service client. Web site hosting cloud servers consume bandwidth for continuous submission.

3.3.1. Malicious SysAdmin

Cloud provider's privileged access to the memory of the VMs sysadmin customer can perform attacks. For example, a system for direct access [Xenaccess] manager provides.

3.4. SLA violation

Cloud machine is misconfigured or corrupt and this is a result of corruption of the data of the customers and to do wrong calculation. Cloud provider to reduce inadvertent customer service performance and SLA (Service Level Agreement) is insufficient for a transaction that violates the can allocate resources.

Attacker to steal valuable data or spam or DoS attacks for the management of the customer's machine in order to seize the customer's software embeds an error. Cloud customers may not be his customers because you lose access to the data or just the data is used in an inappropriate time.

4. DEFENSE STRATEGIES

Address cross-VM attacks approaches are divided into six categories.These categories are; to reduce the success rate of placement, physical isolation applications, the new cache design, in uncertain times to reduce the odds of receiving malicious VM, VM provide for mandatory deterministic leakage enemies, future-proof encryption application cache.

4.1. Placement Prevention

Shared infrastructure, defended at every step in order to reduce the risk of attack. To reduce the success rate of placement, cloud providers will give the authority to put it where the VM users. This does not prevent the brute force attack.

4.2. Co-residency Detection

Cross-VM attacks ultimate solution eliminates co-residence. Cloud customers (especially corporate) even Service Level Agreement (SLA) requires written with physical isolation. But cloud providers are loath to the cloud vendor cost savings and using of cloud sourcing. Cloud providers share infrastructure "VMs, or shared with other reliable infrastructure customers. To ensure the physical isolation, the customers own VMS physical machines' must be enabled in order to verify the private use.

4.3. Trusted Cloud Computing Platform

Present a reliable cloud computing platform (TCCP) provides closed box execution environment for IaaS services. Tccp design goals guarantee the secret execution for virtual machines: 1) to

restrict the execution of the VM in a secure environment 2) is a system administrator with root privileges cannot access a memory VM provides a physical node host. TCCP takes advantage of existing techniques to create reliable cloud computing platforms. These customers are focused on solving problems for data privacy and outsourced cloud computing.

4.4. Defending the New DOS Attack

Migration service called a DOS avoidance strategies have been developed to cope with the new flood attacks. Wide monitoring tool polls by continuous cloud applications and checks whether or not the band resides outside the cloud. When the bandwidth degradation is detected, the process can then be carried out, may temporarily stop the service.
DOS avoidance strategy called immigration service has been developed to cope with the flood of new attacks. A monitoring agent located outside of the cloud applications with continuous probing bandwidth is established to determine whether fasting. When the bandwidth degradation is detected, with the monitoring agent can give temporary service.

4.5. Security as a Service Model for Cloud Environment

Cloud computing security products also benefit from the advantages. Cloud computing allows security products faster, can serve customers more efficiently and effectively. Areas; antivirus, intrusion detection, clearance screening, safety testing, forensic analysis is. Security software is no longer able to get such a service via the cloud.

5. CLOUD SECURITY CONTROLS

5.1. Hacking as a Service

Cloud computing has become an attractive area for cybercriminals. A lot of companies use cloud services have become a target for attackers. Criminals have a variety of attacks to perform and manage the cloud services they use. Services; DDoS, password cracking, and sending spam as
The US National Institute of Standards and Technology (NIST), cloud computing reference architecture. It outlines five major roles: cloud consumer, provider, broker, auditor, and carrier. Cloud paradigm may still be present security challenges require a new application of existing general-purpose set of security controls. So existing security controls for newcomers cloud system cannot fulfill the function anymore. Many basic cloud features, descriptive models and architectural components recommends cloud security issues.

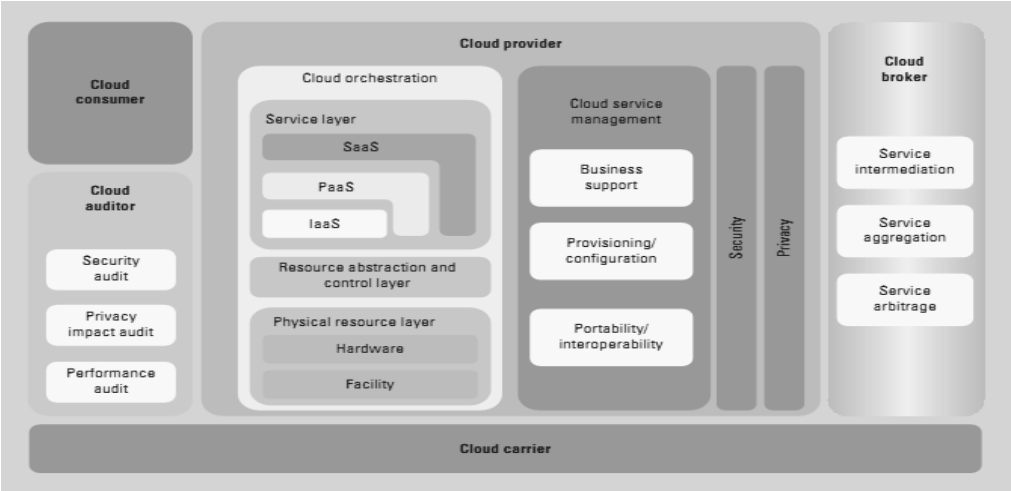

Fig. 1. NIST cloud computing reference architecture. It outlines five major roles: cloud consumer, provider, broker, auditor, and carrier.*)*

5.2. Cloud Brokers

This reference architecture actor implies security composition challenges within composed clouds, such as a SaaS (Software as a service) built on an IaaS (Infrastructure as a service).

5.3. On-Demand Delivery

This feature of the cloud should be easily and instantly deliver safety is already taken. New computer resources being able to get a job associated with the user security issues.

5.4. Resource Pooling

Cloud characteristic manuals are for customers that security resources could allow users to concentrate on a single basket. “Put all your eggs in one basket “This approach shows you the way. Cloud from the perspective of customers, this is a characteristic of the customer mistakenly attacks against the same shared resources using another possibility that may affect the customer reveals.

5.5. Service Models

Paas(Platform as a service), and IaaS(Infrastructure as a service). In addition, the user operations with each other and the cloud itself can attack at a time. There are data multi-tenancy in all the service model.

5.6. Infrastructure as a Service

This service model reveals the challenges with using virtualization as a frontline security defense perimeter to protect against malicious cloud users.

5.7. Broad Network Access

Characteristic of this cloud security is entirely dependent on the network to the service model, probably unreliable makes account for client devices.

5.8. Measured Service

This cloud feature, reveals the need to measure the cloud to encourage the use of public cloud situation.

Conclusions

Use of cloud computing services has been increasing continuously. Like the other cloud computing technologies can be used for good or bad purposes. Organizations that want to move for cloud computing are required to create the transition strategy considering the existing risks. Cloud computing provides convenience to users, but also introduces security problems who were with him.

In this article, Cloud computing's privacy and security vulnerabilities have been what is going on and how to deal. The first count of security vulnerabilities from cloud user's data privacy, so a third party to access the user information means. We have detected against this type of attack and resist systems in our article.

References

[1] P. Mell, "What's Special about Cloud Security?", US National Institute of Standards and Technology, July/August 2012

[2] H. Wang, S. Wu, M. Chen, W. Wang, "Security Protection between Users and the Mobile Media Cloud", IEEE Communications Magazine(references), March 2014

[3] V. Varadharajan, U. Tupakula "Security as a Service Model for Cloud Environment", 2014 IEEE

[4] Hassan Takabi, James B.D. Joshi and Gail-Joon Ahn, "Security and Privacy Challenges in Cloud Computing Environments"

[5] Gail-Joon Ahn, Melanie Siebenhaar, André Miede, Yu-Lun Huang, Ralf Steinmetz, "Threat as a Service? Virtualization's Impact on Cloud Security"

[6] Kui Ren, Cong Wang, and Qian Wang, "Security Challenges for the Public Cloud"

[7] Z. Xiao and Y. Xiao, Senior Member, IEEE, "Security and Privacy in Cloud Computing"
[8] L. M. Kaufman, BAE Systems, "Can Public-Cloud Security Meet Its Unique Challenges?"
[9] G. Peterson, Arctec Group, "Don't Trust. And Verify"