**Journal of Electrical and Electronic Engineering**
2016; 4(6): 145-149
http://www.sciencepublishinggroup.com/j/jeee
doi: 10.11648/j.jeee.20160406.11
ISSN: 2329-1613 (Print); ISSN: 2329-1605 (Online)

# Analyze Threats in Cloud Computing

**Tashev Komil Akhmatovich[1], Islomov Shahboz Zokir Ugli[2], Zokirov Odiljon[1]**

[1]Information Security Department, Tashkent University of Information Technology, Tashkent, Uzbekistan
[2]Cryptology and Discrete Mathematic Department, Tashkent University of Information Technology, Tashkent, Uzbekistan

**Email address:**
k.tashev@tuit.uz (T. K. Akhmatovich), shaxboz4044@gmail.com (I. S. Z. Ugli), z.odil044gmail.com (Z. Odiljon)

**To cite this article:**
Tashev Komil Akhmatovich, Islomov Shahboz Zokir ugli, Zokirov Odiljon. Analyze Threats in Cloud Computing. *Journal of Electrical and Electronic Engineering.* Vol. 4, No. 6, 2016, pp. 145-149. doi: 10.11648/j.jeee.20160406.11

**Received**: October 29, 2016; **Accepted**: November 16, 2016; **Published**: December 21, 2016

**Abstract:** In this work, we conduct an in-depth survey on cloud computing technologies, data storage and information security problems. After an overview of the cloud storage system and threats to them, we focus on four hot data protection topics. They are data integrity, data confidentiality, access control and data manipulation in the secure domain. Also, we describe main threats by services SaaS, PaaS and IaaS in the cloud computing systems.

**Keywords:** IaaS, PaaS, SaaS, SOAP, REST, Private, Public, Hybrid

## 1. Introduction

Modern life supports us computing data and manipulating queries without accessing to physical devices. This method of connection is called cloud computing, also, used devices are called cloud technologies. Cloud computing consists of servers, workstations and telecommunication constructions with connecting global and local infrastructure which includes saving data and information, using high level software and hardware. Cloud computing technologies help to users minimizing expenditures and gives opportunities with working database hardware, appendixes and transmitted data over the network [1]. Cloud computing and storage applications provide users and enterprises with different capabilities to store and process their data in data centers and servers that may be situated far from the user–ranging in distance from across a city to across the world. In very many situations these serves selected by near to users automatically by cloud managers. These technologies direct on sharing of resources to achieve coherence and economy of scale. For using cloud computing resources, we need only connection to the internet and application to contact with users.

## 2. Cloud Computing

Cloud computing, also called cloud technology is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources (e.g., computer networks, servers, storage, applications and services) [1], which can be rapidly provisioned and released with minimal management effort. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers that may be located far from the user–ranging in distance from across a city to across the world. Cloud computing relies on sharing of resources to achieve coherence and economy of scale, similar to a utility (like the electricity grid) over an electricity network.

Virtual computing is not cloud computing, it is a component of cloud computing. Cloud computing is far more than the virtual computing. Simplest form of cloud computing is web applications, web applications are the application which you have use and are created using standard worldwide technology. There applications are created using HTML, CSS, JAVA SCRIPT, XML, PHP etc. When you use these applications you are using applications stored in another server, using web browser installed in your computer. Why this is cloud computing because the application which you are using is no longer installed in your computer, so if your computers stop working then also you can access your data through another computer since your data is still stored in safe place [2].

There are three main services in cloud computing systems:

- SaaS - software as a service source

- PaaS - platform as a service source
- laaS - infrastructure as a service source

### *2.1. SaaS*

Saas allows the use to run the online applications. It is the easiest way of cloud compute. This is for end users. When the software is hosted off-site, the customer doesn't have to maintain it or support it. The idea is that you use the software out of the box as is and do not need to make a lot of changes or require integration to other systems. The provider does all the patching and upgrades as well as keeping the infrastructure running. In some cases you don't have to pay as much up front and you are only billed based on your use of the application. For vendors, SaaS has the appeal of providing stronger protection of their intellectual property as well as creating a continuous stream of income. SaaS applications differ from earlier distributed computing solutions in that SaaS was developed specifically to use web tools, like the browser. This makes them web-native. It was also built with a multitenant back end in mind, which enables multiple customers to use an application.

### *2.2. PaaS*

PaaS supplies all the resources required to build applications and services completely from the Internet, without having to download or install software. Platform as a service sources support web development interfaces such as Simple Object Access Protocol (SOAP) and Representational State Transfer (REST), which allow the construction of multiple web services, sometimes called mashups. The interfaces are also able to access databases and reuse services that are within a private network. Because PaaS is expected to be used by many users simultaneously, it is designed with that sort of use in mind, and generally provides automatic facilities for concurrency management, scalability, failover, and security.

### *2.3. IaaS*

The laaS model provides just the hardware and network. The customer installs or develops its own operating systems, software and applications. The customer does not manage or control the underlying cloud infrastructure but has the control over operating systems, storage, deployed applications, and possibly select networking components (e.g., firewalls, load balancers etc.). Some examples of laaS are: Amazon, GoGrid, 3 Tera etc.

***Table 1.*** *Connection between services and clients.*

| | Cloud Clients |
|---|---|
| | Web browser, mobile app., thin client, terminal, emulator |
| Application | SaaS CRM, Email, virtual desktop, communication, games |
| Platform | PaaS Execution runtime, database, web server, development tools |
| Infrastructure | IaaS Virtual machines, servers, storage, load balancers, network |

### *2.4. Deployment Models of Cloud Computing*

*Private cloud:* Private cloud is cloud infrastructure operated solely for a single organization, whether managed internally or by a third-party, and hosted either internally or externally.

*Public cloud:* A cloud is called a "public cloud" when the services are rendered over a network that is open for public use. Public cloud services may be free.

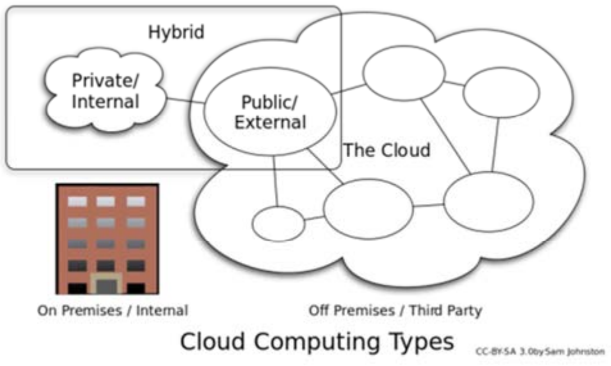

***Figure 1.*** *Models of cloud computing.*

*Hybrid cloud:* Hybrid cloud is a composition of two or more clouds (private, community or public) that remain distinct entities but are bound together, offering the benefits of multiple deployment models. Hybrid cloud can also mean the ability to connect collocation, managed and/or dedicated services with cloud resources.

## 3. Cloud Data Storage Security

The data storage system in a cloud computing center is a cooperation storage service that contains multiple devices and application domains to reduce the operational cost at the client-end and boost overall system efficiency. The basic architecture of a cloud storage system is composed by a storage resource pool, including the distributed file system, the Service Level Agreements (SLA), and service interfaces [3]. Moreover, the architecture can be decomposed into five layers based on their logical function boundaries as shown in Table 2. This layered model shows the delivery flow of stored data in a cloud server.

***Table 2.*** *Cloud storage layered model.*

| Service Interface |
|---|
| Storage overlay |
| Metadata management |
| Storage management |
| Network and storage infrastructure |

Many cloud computing and storage service providers are competing in the market, such as Amazon, IBM, Google, Sun Microsystems, Microsoft, EMC, HP, Symantec, etc. The cloud storage platforms developed by these companies are popular in the Internet such as SkyDrive, Amazon S3, HP Upline, Hitachi Content Platform, etc [4].

Clearly, security in data storage is one of the most important metrics in performance comparison of these cloud computing systems. If the provided cloud storage can be accessed or destroyed by malicious attackers, the service provider will lose trust from its users, and the leakage or full losing of personal data could cause great damage to each individual. When we face to the problem security of cloud storage, just meet with physical and logical security. Physical security ensures by physical devises, such as, tools, access control systems, observation and others. Logical security is constrained with cyber security

### *3.1. Data Integrity*

It is the maintenance of, and the assurance of the accuracy and consistency of, data over its entire life-cycle,[5] and is a critical aspect to the design, implementation and usage of any system which stores, processes, or retrieves data. Data integrity is the opposite of data corruption, which is a form of data loss. The overall intent of any data integrity technique is the same: ensure data is recorded exactly as intended (such as a database correctly rejecting mutually exclusive possibilities,) and upon later retrieval, ensure the data is the same as it was when it was originally recorded. In short, data integrity aims to prevent unintentional changes to information. Data integrity is not to be confused with data security, the discipline of protecting data from unauthorized parties.

### *3.2. Data Confidentiality*

By data confidentiality in the cloud storage system, we mean that the cloud system should protect the data from unauthorized disclosure. The development of new or improved techniques for data confidentiality is one of the major research topics in the field of cloud storage security. The application of cryptographic algorithms to data blocks in the cloud storage is a popular method used to ensure the confidentiality of stored data [6].

### *3.3. Access Control*

One source of cloud security's leakage is caused by malicious service providers. Therefore, access control is used to allow only data owners to access their data. Process allowing to data will be done by authentication: There are three types (factors) of authenticating information [7]:

- something the user knows, e.g. a password, pass-phrase or PIN
- something the user has, such as smart card or a key fob
- something the user is, such as fingerprint, verified by biometric measurement

### *3.4. Data Manipulation in Encrypted Domain*

Instead of focusing on cryptographic algorithms for the data storage security system, there are other research activities that examine the manipulation of encrypted data in a cloud storage system, including data search, computation, and recovery after corruption.

Above given methods or models are used to protect data in cloud computing systems and networks, but there are malicious actions, also called threats that directed to break systems. In our research paper we describe several threats in IaaS, PaaS and SaaS services.

## 4. Cloud Computing Threats

### *4.1. Threat №1: Abuse and Nefarious Use of Cloud Computing*

IaaS providers offer their customers the illusion of unlimited compute, network, and storage capacity — often coupled with a 'frictionless' registration process where anyone with a valid credit card can register and immediately begin using cloud services. Some providers even offer free limited trial periods. By abusing the relative anonymity behind these registration and usage models, spammers, malicious code authors, and other criminals have been able to conduct their activities with relative impunity. PaaS providers have traditionally suffered most from this kind of attacks; however, recent evidence shows that hackers have begun to target IaaS vendors as well [8]. Future areas of concern include password and key cracking, DDOS, launching dynamic attack points, hosting malicious data, botnet command and control, building rainbow tables, and CAPTCHA solving farms.

### *4.2. Threat №2: Insecure Interfaces and APIs*

Cloud computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. Provisioning, management, orchestration, and monitoring are all performed using these interfaces. The security and availability of general cloud services are dependent upon the security of these basic APIs. Attacker takes access to the system by authentication or access control devices, also, security software and hardware which directed to protect information in the cloud storages. Furthermore, organizations and third parties often build upon these interfaces to offer value-added services to their customers. This introduces the complexity of the new layered API; it also increases risk, as organizations may be required to relinquish their credentials to third parties in order to enable their agency.

### *4.3. Threat №3: Malicious Insiders*

Malicious actions direct against cloud computing systems - is the most abundant in its classification of the list of crimes. These include:

- Penetration into the system via an external (eg, telephone) communication channel with the assignment of powers of one of the legitimate users for the purpose of counterfeiting, copying or destruction of data. Implemented by guessing passwords or selection, identification of passwords and protocols through agents in the bank, intercepting passwords when connecting to a tacit channel during communication, remote interception of passwords as a result of the reception of electromagnetic radiation;

- Penetration into the system via the telephone network when rewiring channel to the attacker's modem after entering a legal user to the cloud and the presentation of its powers for the purpose of assignment of the rights of the user to access the data;
- Copy of the financial information and passwords in collusion passive connection to the cable network or receiving electromagnetic radiation network adapter;
- Analysis of the traffic in the passive connection to the communication link or the interception of electromagnetic radiation detection equipment for the communication protocols
- Lock the channel's own messaging communication, causing a denial of service legitimate users.

### *4.4. Threat №4: Shared Technology Issues*

IaaS vendors deliver their services in a scalable way by sharing infrastructure. Often, the underlying components that make up this infrastructure (e.g., CPU caches, GPUs, etc.) were not designed to offer strong isolation properties for a multi-tenant architecture. To address this gap, a virtualization hypervisor mediates access between guest operating systems and the physical compute resources. Still, even hypervisors have exhibited flaws that have enabled guest operating systems to gain inappropriate levels of control or influence on the underlying platform [9]. A defense in depth strategy is recommended, and should include compute, storage, and network security enforcement and monitoring. Strong compartmentalization should be employed to ensure that individual customers do not impact the operations of other tenants running on the same cloud provider.

### *4.5. Threat №5: Data Loss or Leakage*

Most business organizations is accompanied by supporting complex cloud computing systems and centralized storage, in one way or another already implemented information security. Work with files stored in a vault is often uncomfortable, so users often copy the files from the cloud storage systems and storage to your workstation, or external media. These actions are often justified by the speed of the access/processing, convenience, necessity of working out of the office, business trips, etc., accompanied by a phrase such as “It's easier and more convenient”. At this time third party, also called hackers try to access to the data which transmitted over the network. Not only data, they can loss encryption and decryption keys. Loss of an encoding key may result in effective destruction. Finally, unauthorized parties must be prevented from gaining access to sensitive data.

Also, Data loss can be linked to human error (such as customer and supplier), the use of unreliable drives and media, due to the loss of the encryption key, and also due to the unreliability of the data center equipment or lack of disaster recovery procedures.

### *4.6. Threat №6: Account or Service Hijacking*

Prices hacker is a pretty significant list, but the most expensive is considered theft of bank account and all the data on the debit card. This service will cost an attacker just a few hundred dollars. At the same time they will receive more and associated services in the form of cards with a magnetic strip for only some ten dollars or a little expensive, twenty, but chip card. All accounts are protected by IP logon passwords, and even cracking the account, the attacker will not have time he borrowed it, because He is locked in a very short time, and benefit from the account for a few hours. Loads DDoS attacks - is an artificial load on the site server [10], as a result of which, the site ceases to function normally and starts very slow and be inaccessible to most users.

### *4.7. Threat №7: Unknown Risk Profile*

Vulnerabilities in the API are usually associated with their refining service providers. This is done in order to provide additional services, but the side effect is to increase the complexity of the API and various risks. This risk applies to all types of services, including SaaS, IaaS and PaaS. As countermeasures recommended tools such as analysis of security APIs approaches, providing strong authentication and access control, the use of means of traffic encryption, as well as analysis of the dependency chain associated with the API. Activities of the company's employees, the service provider can also be a threat. This is due to the concentration in one place of the set of IT services, operating under a single management for the benefit of different customers, and supplier processes and procedures are often not transparent to its customers. At the same time the staff has full access to data and other resource providers, which creates the risk of unauthorized access, and to detect it may be difficult or even impossible. This risk also applies to all types of services, including SaaS, IaaS and PaaS.

***Table 3.*** *Threat identifications in IaaS, PaaS, SaaS.*

| Threats/Services | IaaS | PaaS | SaaS |
|---|---|---|---|
| Threat №1 | + | + | |
| Threat №2 | + | + | + |
| Threat №3 | + | + | + |
| Threat №4 | + | | |
| Threat №5 | + | + | + |
| Threat №6 | + | + | + |
| Threat №7 | + | + | + |

## 5. Conclusions

Cloud computing systems are widely used in all fields of information technologies, therefor development efficiency and security cloud computing architecture is actual problem. Also, in this paper was considered cloud computing and storage, its security, services, models, data protection topics. By reviewing security parameters were given analyzes threats and shown as a seven main threats. These threats were analyzed by IaaS, PaaS and SaaS services and given as a table 1. By those table threats 2, 3, 5, 6, 7 influence all services, threat 1 IaaS and PaaS and threat 4 only for IaaS.

## References

[1] Hassan, Qusay. “Demystifying Cloud Computing”. The Journal of Defense Software Engineering. CrossTalk. 2011 (Jan/Feb): 16–21. Retrieved 11 December 2014.

[2] Vigya Dubey, Pranjal Agrawal. “Cloud Computing and Data Management”, Symposium on Colossal Data Analysis and Networking (CDAN). 2016.

[3] W. Zeng, Y. Zhao, K. Ou, and W. Song, “Research on cloud storage architecture and key technologies" in Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human, Seoul, Korea, 2009, pp. 1044-1048.

[4] Chun-Ting Huang, Zhongyuan Qin, Jay Kuo. “Multimedia Storage Security in Cloud Computing: An Overview”. MMSP 2011. IEEE. 2011.

[5] Saakshi Narula, Arushi Jain, Ms. Prachi. “Cloud computing security: amazon web service”. 2015 Fifth International Conference on Advanced Computing & Communication Technologies.

[6] Akanksha Singh, Smita Sharma, Shipra Ravi Kumar, Suman Avdesh Yadav. “Overview of PaaS and SaaS and its Application in Cloud Computing”. 2016 1st International Conference on Innovation and Challenges in Cyber Security (ICICCS 2016).

[7] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “Above the clouds: a Berkeley view of cloud computing” Univ. of California, Berkeley, CA Technical Report No. UCB/EECS-2009-28, 2009.

[8] Boritz, J. “IS Practitioners' Views on Core Concepts of Information Integrity”. International Journal of Accounting Information Systems. Elsevier. Retrieved 12 August 2011.

[9] A. Yun, C. Shi, and Y. Kim, “On protecting integrity and confidentiality of cryptographic file system for outsourced storage” in Proceedings of the ACM workshop on Cloud computing security, Chicago, Illinois, USA, 2009, pp. 67-76.

[10] “Micro Strategy’s office of the future includes mobile identity and cyber security”. Washington Post. 2014-04-14. Retrieved 2014-03-30.