International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2019): 7.583

Cloud Computing Security Issues and their Data Privacy Concerns

Amal Matrouk Aljohani

Syracuse University, Syracuse, United States

Abstract: ***After the invention of cloud computing technology, the concept of building computer system with unlimited resources becomes more simplified. With cloud computing, business owners, can manage and share their information through business organization from anywhere twenty-four hours a day. Organization and business area which are using cloud services must be aware of their information policy, involving data privacy, reliability and security. Building cloud computing system will expose their information that are accessed by authorized people to hazard if they did not build strong secure system to increase their security level and protect it by authorizing only people who need to access them. The goal of this research paper is to give short vision of cloud computing concept by identifying their different types and discuss cloud security main issues to attract both users and business owner attention to the potential risks of sharing their important data through cloud system without knowing security limitations for each model and secure their system by overcome potential threats for their cloud system.***

Keywords: Attacks, Cloud Security, Cloud Attacks, Cloud Privacy, Security and Privacy in Cloud, Security Analysis on Cloud, Cloud Deployment Models, Cloud Characteristics, Data Privacy

1. Cloud Computing Overview

In this section, we will provide clear view on the concept of the cloud computing system and simple description on its different types. If we notice as shown in the diagram below the cloud is used to represent the internet. Computer engineer and designer used cloud to differentiate it from other component and there is nothing to do with the weather or clouds. The system named as a cloud computing due to the importance of the network to all connected devices and resources within the system. As it shown in figure 1-1 internet is the basic component in the cloud computing service and it represented as a cloud [1].

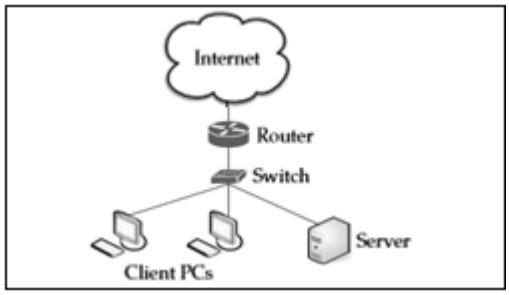

Figure 1-1: A cloud is used in network diagrams to depict the internet

Cloud computing system constructed in such a way to allow you to access applications located in different location specifically another computer or internet device. There are valuable benefits from using cloud system especially for companies which contain several computers that need installation of software. It will be costly if the company install the software for each computer and pay for them separately. In addition, they need a lot of equipment to make their computers work successfully. However, after the invention of cloud computing service this work can be done in an easy way. They can host another company which can provide them with specific service that meet their needs for all computers through the network. Consequently, they will save companies' budget since they don't need to pay for maintenance and efforts. Figure 1-2 show the basic concept for this system, the connection between the company and the service provider illustrated as a cloud [1].

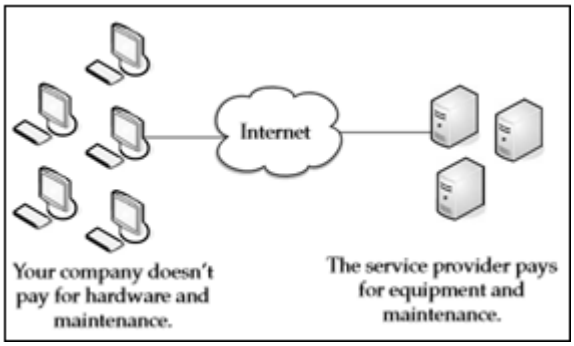

Figure 1-2: With Cloud computing, other companies host your applications.

1.1 Cloud Computing Services

By using cloud computing services users can gain the following benefits:

- Scalability which means the system will perform with the same efficiency even if the workload for the system expanded.
- There are no high berries for cloud service which allow small business to take advantage of their services.
- Hardware and devices are independent from each other; as a result users can access their system from different hardware anywhere.
- It allows many users to share available resources.

1.2 Types of Cloud Services:

1.2.1 Software as a Service (SaaS): In this model, customer can access hosted application through the internet. As a result, the customer doesn't need to keep the application running or fix it in case it has some issues. They don't need to worry about services maintenance any more. On the other hand, since the software out of their box customers are not authorized to make any changes in the software. In addition,

they have to accept any change when the hosting company decides to modify the services [1].

SaaS Benefits: The biggest advantage from using this model is saving money since the hosting application will cost less money instead of buying the whole application. Service provider can offer you more reliable applications which are cheaper than buying them as a package with serial number for every single computer. Another advantage we must take it in our account is the maintenance of the software, since service provider are responsible to keep system running and check them periodically companies do not need to worry about maintenance. Consequently, they do not need to hire IT specialist which also affect positively in their budget and employees needed offices. In addition, service provider can easily customize applications upon customers' requests which is not easy to be implemented by users who do not have full comprehensiveness to modify the code. Moreover, Security Secure Sockets Layer (SSL) are used in SaaS and allows users to access their applications securely without any need to use more complex configuration such as , virtual private networks to secure their applications. Finally, the qualities of the services and the bandwidth have increased in recent years this feature allowed users to access their applications with high speed and low latencies [1].

1.2.2 Platform as a Service (PaaS): Platform as a Service (PaaS) is a collection and variation of SaaS [2]. It is also named cloud ware, in this model all resources which are required to install services and desired applications supplied via the internet by service providers, the company doesn't need to install any software. PaaS services include development, application design, deployment, hosting and testing. In PaaS providers are not familiar in communicating with each other, as a result it is difficult to change to another service provider. If the user decided to do so, he needs to pay more money. Another weak point, is that all data in user's applications will be lost if the business goes down [1].

In (PaaS) model, the vendor who provide service environment offers application developers, who are responsible to develop applications and offer applications services via the provider's platform. Then services provider will develop specific standards for the development, and channels to distribute required services and payment to their clients [2].

The biggest benefit from using PaaS systems is that companies can start their web based applications with the minimum cost and complexity because they do not need to buy huge servers and setting them up by IT specialist [2].

1.2.3 Infrastructure as a Service (IaaS):
In IaaS application model, service providers host the entire infrastructure for clients to run their applications. The IaaS model provide specific utilities to customers who are responsible to pay for the amount of resources they used such as disk space, processing power and any other resources that customers actually consumed. The users in this model abstracted from infrastructure details, including location, scaling, backup, physical resources, security and so on. In this application model, service providers have a complete control of the entire infrastructure. On the other hand, clients can decide and control of the infrastructure location and what required services should be run on each server. In addition, service providers can extend their services and add more capacity in order to meet their customer's demand [2].

Infrastructure as a Service (IaaS) Disadvantages

- The business or organization is responsible for software upgrading.
- The maintenance and infrastructure is also the responsibility of the organization.
- When the organization want the hardware to be of a unique type or the software to be edited to support the application they will pay for required change.
- The security issues and features of the IaaS Cloud Service Provider may not be adequate for clients' needs.
- In case the customer need to connect between their internal software and different software in another Cloud system the internet connection supported by cloud provider may not be adequate for the speed that client's connections required [4].

1.3 Essential Cloud Characteristics

The US National Institute of Standards and Technology (NIST) provide description of cloud characteristics which are as follows [3]:

- **On-demand self-service.** This means that clients can directly manage or order services without any need to human interaction with the company or service provider.
- **Broad and ubiquitous network access.** Cloud services can be accessed via the internet using specific standard protocols and mechanisms.
- **Resource pooling.** Provided cloud service used computing resources which are realized through using a homogeneous infrastructure which are shared among all service clients.
- **Rapid elasticity.** Scalability of resources which means that resources are scaled down and up elastically.
- **Measured service**. Service and resources usage are measured and service providers support optimization of their resource. The customers will pay depending on their consuming on resources.

As mentioned above these are essential five characteristics for cloud computing, see figure 1-3 [5].

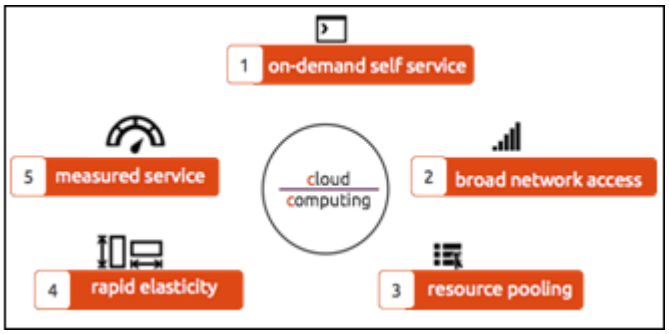

Figure 1-3

2. Security Issues in Cloud Computing System

In order to make our system secure we need to look at different levels in which security is required on them. These levels including Internet, program, server and database access security. Also, data security and privacy must be taking into our account under security umbrella since all business owners share their sensitive data and information through cloud system.

2.1 Basic Criteria for a Secure Cloud System

In order to have a good and secure cloud computing system, service providers ought to have a good policy to secure data and make sure that all shared information safe enough from any vulnerabilities and hazard. Integrity, confidentiality, availability, data sanitization and physical security are the most important requirements for secure system. To clarify and understand these requirements we will define each keyword separately [6].

Integrity: Integrity related to the information that goes through the system. Service providers must ensure that all data and information which located in a system, is a correct representation of the intended information and did not modified or changed by unauthorized users.

Confidentiality: Making sure that data is not exposed to unauthorized groups.

Availability: Making sure that information availability is not affected by malicious or improper actions.

Data sanitization: Data sanitization is the process in which all sensitive information must be removed from storage devices to ensure its security and protect them from being shared through the system by unauthorized users.

Physical security: It is related to hardware security that means ensuring that all connected hardware is authorized to have access to data center. When some clients or users are not interested to have their cloud system due to closing their business or any other reason, their connected resources must be removed immediately to keep the security level up.

Overall the physical security level is acceptable and it developed so quickly day after day. However, our big concerns are software security, because we still need to improve software security level to make sure that our sensitive software secure against malicious viruses and hackers. It is kind of challengeable for cloud service developers to enhance and develop software security due to the amount of threats that increase vastly every day [6].The security level of the cloud system can be managed by the way of the cloud is building. Some deployment provides less level of security than others for example public cloud system which offer service for multiple customers and organizations. Consequently, clients have less control over the whole infrastructure since it controlled by the service providers. In short words, this option will be less sufficient to organizations which are concerning more about their privacy and information security.

2.2 Cloud Deployment Models

As stated below there are four different cloud deployment which are Public cloud, Private Cloud and Hybrid cloud.

Public Cloud: This infrastructure allows many users to have connection on it. In other words, several organizations are able to work on the same infrastructure simultaneously. This cloud system is managed and hosted by the service provider. Hosted company is responsible for maintenance, management and installation. The biggest advantage is that clients are only pay for their resources that in use. Consequently, the cost will be eliminated. Because customers have limited control on the infrastructure and restricted from optimizing their cloud system the security level will goes down comparing to private cloud system [7].

Private cloud: This cloud model owned and managed by the business or organization for this reason it will be more secure comparing to public model cloud. On the other hand, it is more expensive. Service providers allow clients to have control the infrastructure in order to improve their security but this feature is not presented in public cloud. Moreover, there is no restriction or regulations on bandwidth or security as in a public cloud; users can optimize their system to meet their needs which count for their privacy level [7].

Hybrid Cloud: Hybrid means collection of two or more cloud models which are connected in a specific way that allow data to be migrated between them without conflicting each other. This type of clouds deployment is built by the hosted company and responsibilities in management are divided between cloud provider and clients. To meet customers' needs an organization can write down their needs and goals in services that they want. This construction is more useful since it provides more security level than other deployment types. The biggest disadvantage of hybrid cloud is the complexity of building them. It can be act as public, private or community depending on the way we construct them. In addition, services which are coming from different sources must be treated as it comes from specific location. Moreover, the interaction between public and private components will cause conflicts on implementation. This model should be constructed well under the supervision of qualified experts. Otherwise, it will cause problems in both implementation and security [7].

3. Security Analysis on Cloud Computing Services

As we discussed in section 1 there are three types of services which provided to cloud customers Platform as a Service (PaaS), Software as a Service (SaaS) and Infrastructure as a Service (IaaS). Now we will discuss the security issues of these types of service. According to the study and analysis done by Keiko Hashizume1, David G Rosado2, Eduardo Fernández-Medina2 and Eduardo B Fernandez researchers on security concerns for Cloud Computing, there is a list of threats and vulnerabilities that can affect cloud models. Researchers provide a survey on these potential threats by listing them and finding the relationship between them [8].

Table 1 Summary of the topics considered in each approach

Topics/References	[4]	[6]	[10]	[16]	[17]	[18]	[19]	[20]	[21]	[22]	[23]	[24]	[25]	[26]	[27]
Vulnerabilities		X		X	X	X	X	X	X			X			X
Threats		X		X	X	X	X	X	X	X	X	X	X	X	X
Mechanisms/Recommendations	X			X		X		X				X	X	X	X
Security Standards							X			X					
Data Security	X		X				X		X		X		X		X
Trust			X								X		X	X	X
Security Requirements	X		X						X		X			X	X
SaaS, PaaS, IaaS Security					X				X			X			

Table 1 analyze and identify list of vulnerabilities and threats which found on Cloud Computing. The studies focus on potential threats and risks and give some recommendations that help cloud service providers to avoid and cover from these malicious threats. In the research, they discuss other topics which are related to security issues in the Cloud system such as security recommendations and data security.

In order to discuss the security issues for each model first we need to be aware of the relationship between these types of services. Both PaaS and SaaS hosted above IaaS which means any impact on IaaS will lead to breach SaaS as well as PaaS and vice versa. These dependencies between cloud services models increase potential risks on security of the cloud system. Each model has it is own security which deployed by service providers but the combination of these security for each cloud model may cause conflicts for the combined cloud.

3.1 Security Issues in Software-as-a-service (SaaS)

As we mentioned before SaaS service providers give their clients chance to access services depend on their needs and request. We discussed this model in details and we know that SaaS customers have limited control on the security level between all available cloud models in the system. Consequently, SaaS applications will have more security concerns than other applications [8].

3.1.1 Applications and Data Security

The study and research argues that applications which are provided through the internet and web browser in SaaS expose the security of applications to many risks. Application's security did not protect them from being attacked by hackers who use web service and malicious software on the internet. According to The Open Web Application Security Project (OWASP) there are ten critical web security threats which must be taken into our account to avoid security risk and secure our applications which served on the web. In addition to application security data security very sensitive for any organization. It is very challengeable to secure data in SaaS due to customer's limited control over the security and infrastructure of their service. In this cloud model service providers are responsible of securing customer's data. Another point which is very critical for organizations is data backup in case of disaster. On some situation service providers, can limit their services on the cloud or maybe they stop their business which put organizations in a bad situation due to their stored data in service provider's datacenter.

3.1.2 Applications Accessibility

Applications on SaaS can be accessed from any computer or mobile devices since applications are available on the network. As a result, this will increase security risks due to using insecure Wi-Fi or stealing information from mobile devices.

3.2 Security issues in Platform-as-a-service (PaaS)

In this model two security levels are presented which is the security of the platform itself and the security of user's applications that deployed in the PaaS. Service providers are responsible to secure the platform and make sure that runtime engine operate client's applications correctly. PaaS as well as SaaS cause some issues in data security [8].

3.2.1 Infrastructure Security

Because users do not have authority to access specific layers, service providers must insure that infrastructure is secure enough as well as user's applications. It is true that users in PaaS can control the security of their applications but they do not have wide knowledge to assure that their environment is secure.

3.2.2 The relationship of Third-party

PaaS provide Mashups service which is located under third party web services. This service combines and associate number of sources into a single unit. That means security issues will increase due to data security and network security which are related to mashups feature. In short, PaaS security depends on both web security and third party services security.

3.2.3 Application Life Cycle

PaaS users and developers must be aware of their application's security level when they need to upgrade their applications. IT specialist need to make sure that development processes are adapted to accommodate required changes without any conflicts with application's security. In addition, developers and IT specialist have to understand data illegal issues to stand away from them. Data must be store in legal locations that insure its security and privacy.

In conclusion, since data is transferred, processed and stored in the application deployed in the cloud system,

data security is the biggest concern in both SaaS and PaaS models.

3.3 Common Security Risks in Cloud Computing

Despite many advantages of cloud computing such as eliminate the cost and the space for business and organizations. Many business stay away from adopting their services on the cloud system due to their concerns in the privacy. Due to the fact of sharing resources among number of users through the internet in cloud models, there are number of threats and breach which weaken cloud security.

As shown in figure 1-4 different types of common breach that threaten cloud security. According to this statistics theft represent the largest percentage among other breaches such as unauthorized access, loss of data, hacking and improper disposal.

Attacked web applications by hackers can cause loss of sensitive data. On the other hand, data breach can be occurred when someone trying to access this data without any permission -unauthorized users-. As we discuss above cloud computing allow many business and organizations to share the same resources via the internet which lead to increase the risk of their processing data. In this situation, the risk of data misuse will be high. Several accidental transmission issues or insider attack could also lead to data breach [9].

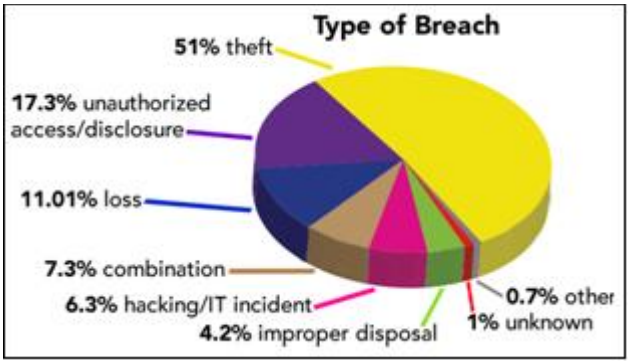

Figure 1-4

3.4 Five Important Things to Secure the Cloud System

These following tips are important to be considered when we want to build our system with acceptable security level [10].

1) **Where is data located:** If you have no idea about the location of your data then you cannot secure your system. You should be aware where your data is saved and stored. After that you can apply some tools on data to upgrade its security. Virus detection firewalls and data encryption will increase the data security and protect them from being accessed by unauthorized persons.
2) **Backup your data:** In both SaaS and PaaS models data may be lost at any time the service providers decided to stop providing their services. So, whatever happens makes sure you have a copy of your data. This will secure your business and organization not only the data.
3) **Data center security policies:** You must know the server and data center in which your data will be stored. Consequently, you will know your data policies according to the server type and applicable services in this server.
4) **Ask your clients for references:** Asking other client who takes advantage of this cloud system will provide you with their recommendations that will help you to take advantage of their experience in securing their data.
5) **Testing the system:** Testing your system security by trying to access data while you are unauthorized to access them will give you tip about your data security level because if you find some way to access data, someone will find this way too. In addition, you need to scan it periodically to get rid of malicious software and viruses.

In conclusion, it is not easy to secure the cloud system, we can upgrade the security level and secure our data but it is not guarantee to protect this data from any breach 100%. On the other hand, private cloud gives more security than public framework.

4. Conclusion and Future Work

Since I had limited time and space I could not include more analysis that weakened cloud system security. There are different surveys and researches that argues data which are stored in the cloud datacenter is in high riskfor unauthorized access.

According to what we discussed, cloud computing still need to increase the level of security for business and organizations. They need to adopt more powerful tools and software to overcome potential threats raised through the network. Service providers have to be aware of different types of risk and breach which threaten their services; They should educate themselves to get rid of these breaches in powerful way. Hacker's methods are increasing vastly day after day. As a result, data became more critical and need to be protected enough from being breached. Service providers can work with well-educated developers to adopt new architecture in which data security is the first priority.

It is true that there are a lot of benefits from using network hierarchy but it makes accessing data easier for hackers through the internet. If we want to provide strong security, we need to put efficient policies on the network and narrow it to prevent unauthorized users from accessing it. Today, architects are interesting in developing communication architecture which will affect positively on cloud computing security. Architects can employ another way for connecting devices and servers in which network connections become more secure for customer's use only. This method will minimize huge number of threads especially unauthorized people.

In conclusion, since cloud computing servers and datacenters located away from customers and allow multiples access for different users at the same time security issue must be concerning for any business or company that take advantage of cloud services.

References

[1] Anthony, T., Toby, J & Elsenpeter, R. (2010), *Cloud Computing a Practical Approach.* Retrieved from http://www.unde.ro/zoran/papers/citations/CloudComputing.pdf
[2] Mather, T., Kumaraswamy, S & Latif, S. (2009), *Cloud Security and Privacy an Enterprise* Perspective on Risks and Compliance. Retrieved from http://www.di.fc.ul.pt/~nuno/PAPERS/security3.pdf
[3] GroBauer, B., Walloschek, T & Siemens, E. Understanding Cloud Computing Vulnerabilities research paper Retrieved November 17, 2016, from http://www.service-architecture.com/articles/cloud-computing/infrastructure_as_a_service_iaas.html
[4] Retrieved November 18, 2016, from http://www.vyomtech.com/2013/10/30/what_is_cloud_computing.html
[5] Karahroudy, A. (2011) Security Analysis and Framework of Cloud Computing with Parity-Based Partially Distributed File System. Masters Thesis, East Carolina University. Retrieved from
[6] http://thescholarship.ecu.edu/bitstream/handle/10342/3630/AsgharyKarahroudy_ecu_0600M_10476.pdf?sequence=1
[7] Padhy, R. Patra, M & Satapathy, S. (2011). Cloud Computing: Security Issues and Research Challenges. Retrieved from http://ijcsits.org/papers/Vol1no22011/13vol1no2.pdf
[8] Hashizume1, K., Rosado2, D., Fernández-Medina2, E. & Fernandez, E. (2013)
[9] An analysis of security issues for cloud computing Retrieved November 20, 2016, from https://www.computer.org/web/the-clear-cloud/content?g=7477973&type=blogpost&urlTitle=analyzing-security-concerns-with-cloud-computing-and-discovering-solutions
[10] Retrieved November 23, 2016, from http://www.onlinetech.com/resources/references/top-5-tips-for-cloud-computing-security