A STUDY OF INFORMATION SECURITY AND SECURITY INSURANCE OF CLOUD COMPUTING IN THE WORLD OF TECHNOLOGY

Leelavathi Rajamanickam[1,*], Rajamohan Parthasarathy [2]

[1]*Center for Software Engineering, SEGI University, 47810 Selangor, Malaysia*

[2]*Center for Network Security and IOT, SEGI University, 47810 Selangor, Malaysia*

[*]For correspondence; Tel. + (60) 03-6145 1777, E-mail: leelavathiraj@segi.edu.my

ABSTRACT: *As the paper describes the basic characteristics of cloud computing. As a result of research processing in the computing field, there have three types of cloud computing models such as cloud computing, parallel computing, and grid computing. Cloud computing used to be a new way of providing facilities through the internet and computers. The main goal of cloud computing is to produce a system with all facilities minimum cost and base structure. Information security and security insurance are the two basic elements for the customer to worry about cloud innovation. Although many strategies on the concepts of cloud computing have been researched in the two sectors, such as education and enterprise. Information security and security assurance are arriving up to more needed for the progress of cloud computing in business sectors, government agencies, and industrial revolutions. Information security and security insurance topics are applicable for resources and programming in the design of the cloud. In this paper, we state a homogenous study on the current scenario with respect to the information security and protection insurance policies used in cloud computing.*

Keywords: cloud computing; security, privacy, and data integrity

1. INTRODUCTION

Cloud computing is a new way of providing internet facilities via the internet and computers. Cloud computing is based on service offering or pays according to the usage of the internet by not referring to any of the hardware or the resources. Cloud computing is stated as a computer model that is made on the required basis, that allows quick and easy access, from a network to a common storage computing repository (e.g. servers, database, networking, repository, facilities). Cloud computing applications can be broadly classified into three areas known as cloud delivery models: Infrastructure as a service (IaaS), Platform as a service (PaaS), and Software as a service (SaaS) [6]. This paper discusses the attributes, service model, deployment model, privacy, and security issues present in cloud computing architecture with the required output. Cloud computing has features such as availability of the resource, easy maintenance, dynamic computing approach, service-centric approach depending on the model, least or individual-managed platform consumption-based billing. Securing data has been a big challenge in information technology and it has been a severe issue in the environment of the cloud as the data is distributed to various systems. In traditional systems, data security is much easier than compared with cloud computing.

1.1 Dynamic computing infrastructure:

Systems are placed remotely and maintained by certain organizations to perform task for businesses, companies, and industries in finding out the required resources to operate. The foundation for the dynamic infrastructure is done or made to look the same way every time, able to be made bigger or smaller and secure physical infrastructure. There should be a level of unnecessary thing to secure high availability, but in most cases, it must be easy to scale because growth demandeds for growth without the need for redesign. Next, it must be virtualized [7].

1.2 IT service-centric approach:

Cloud computing is centered on IT (or business) services. By abstracting a view of server-centric, clients or users can access easily the efficient, assumed conditions prepared for the facilities. The information technology enables users to adopt a service-centric approach and flexible athletic capability for business– allowing users to complete a task more easily and quickly, making business easier, reducing costs, or increasing the money income [7].

1.3. Self-service based usage model:

The benefit that is often ignored from the service provider's point of view is they facilitate more self-services giving users and less time management. This actually saves in terms of time and money; this allows managers to concentrate on higher-value tasks [7].

1.4 Deployment models:

Businesses can choose from public, private, or Hybrid clouds or community clouds. Below are some fundamentals of each to help with the decision-making process [8].

Public cloud: A Service provider who hosts the infrastructure makes it available to the public. Public cloud provides like Amazon Web Services and Alibaba Cloud have their own infrastructure operating and can be accessed over the internet. The features of the cloud system purchased and operated by academicians, governments, industries, businesses. Clients or users do not have control on visibility or facility available the model as they are sharing the same infrastructure pool with limited configuration.

Private cloud*:* The services that are offered either through the internet or any internal network that is dedicated to a single organization. It facilitates organizations to broadcast to the cloud in specifying the information with respect to safety and control and there is a lack of not sharing in a public cloud environment. It will be broadcasted by the managers or by third parties.

Hybrid cloud: The cloud environment with a combination of two or more cloud services. The aim is to provide a managed environment. The combination can be a private cloud or public services that make a unique entity, they are combined together for multiple deployment models. In this model, the use of infrastructure is partial or full, from the cloud provider. Data and application portability can be joined by a standard or patented technology. Private cloud is usually associated with public clouds where else, large organizations are usually benefited from a private cloud. The evolution of cloud computing in business will continue to evolve based on the four major paradigms.

Community cloud: Thefacili cloud infrastructure is shared among specific communities of consumers from an organization that has the same concerns. It can be owned and operated by one or more of the organizations in the community or a third-party service provider on or off-premises. Community clouds are a mixture type of private cloud built and operated for specific communities.

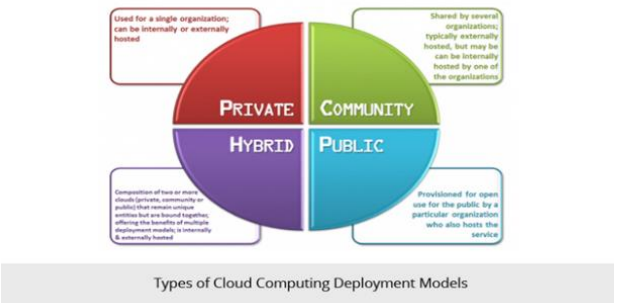

Used for a single organization; can be internally or externally hosted
Shared by several organizations; typically externally hosted, but may be can be internally hosted by one of the organizations
PRIVATE
COMMUNITY
HYBRID
PUBLIC
Composition of two or more clouds (private, community or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models; is internally & externally hosted
Provisioned for open use for the public by a particular organization who also hosts the service
Types of Cloud Computing Deployment Models

Fig (1). Types of cloud

2. SECURITY AND PRIVACY IN CLOUD COMPUTING

This segment addresses the deep part of this topic in terms of safety and protection in cloud distributed computing. The security issues for cloud computing vary depending on the databases, models, framework, asset planning, control, and administration. Consequently, privacy in cloud computing transforms the issues for frameworks to a convincing number. For example, the framework of the cloud system that interconnects should be secure. The physical and virtual machine mapping should be done securely.

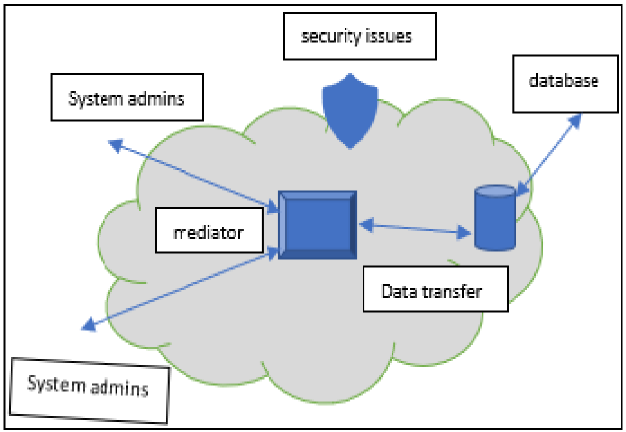


Fig (2). Security issues in cloud

Referring to Fig 2 above, there are six specific areas of the cloud computing environment where equipment and software require substantial security attention [5]. These areas are: (1) security of database at rest, (2) security of data transfer, (3) system admins/users/applications/processes, (4) security mediator between data belonging to different customers, (5) cloud legal and regulatory issues and (6) incident response.

Security of Data: *The* security of data can be done through the encryption process cryptographic encryption components are surely the best alternatives. In spite of the fact that product encryption can likewise be utilized for ensuring information, it makes the procedure slower and less secure since it may be possible for an adversary to steal the encryption key from the machine without being detected.

Data transfer: Encryption is the best alternative for securing information in transit too.

Authentication: In addition, authentication and integrity protection mechanisms ensure that data only go where the customer wants it to go and it is not modified in transit. The trusted computing group's (TCG's) IF-MAP standard takes into consideration ongoing correspondence between a cloud specialist co-op and the client about approved clients and other security issues.

Mediator between customers: One of the more obvious cloud concerns is a separation between a cloud supplier's clients (who may be competing companies or even hackers) to keep away from accidental or deliberate access to delicate data.

Legal and legal and regulatory issues: Legal and regulatory issues are critical in distributed computing that have security suggestions. The legal issues are to be considered to include the security of data and transfer the data to the systems with all legal regulations with respect to the terms.

3. PROCESS REVIEW

Observation:

Based on the study conducted on the cloud service provider “Perfect Cloud”, it is observed that they give supreme affirmation that regardless of whether an assailant was to enter a server they could never have enough data, regardless of whether effectively taking information out of memory, to ever reconstitute a key or take an online character.

Data breaches:

Accessing data with authorization, this leads to data manipulation and damage the data. Data breaches affect businesses, organizations, governments, and industries. This is either by the network or somebody who uses your system or phone or laptop. Find what was the data stolen and take the necessary action, protect the systems with strong passwords. [2]. An information break happens when a programmer makes, uses, or discharges delicate data. Information ruptures additionally happen when a hapless person commits an error and unintentionally opens an information to unapproved watchers [6].

Data Loss:

The data loss is a human error, it is an error in the information that is being destroyed by negligence, mishandling of data, storage error, virus, etc., Backing up data, encrypting the information, have anti-virus, and protecting the address of storage helps in securing data. [8]. It is the fault of human mistakes to lose the data. Information technology should be secured by setting up regular security checks and encrypt the data or by changing the passwords or keeping a master list to secure the information. [6].

So, there can be a loss of data due to the attackers. The loss of data can be through a natural disaster, malicious attack, or wipe out data by the service provider. But this is the responsibility of cloud providers to protect the information or data by encrypting files in case of accidental data exposure.

Insufficient due diligence

It can represent a security hazard, an organization enters the cloud without permission of the above, that the system will not cooperate with the requirements. [5].

An organization must find a suitable service and the service must be expected by the clients. For example, reasonably expect and how much you pay for what you need.

Hijacking of account

The usage of cloud in various organizations has developed an issue in organizing the record capturing. Aggressors presently can utilize your (or your employers) details to log in remotely and can get the required information and use it. Moreover, attackers can twist and control data through commandeered accreditations. Different strategies for seizing incorporate scripting bugs and reused passwords, which enable assailants to effectively and regularly without location take certifications [5].

Cloud-based records are no exemption. Organization solid two factor verifications and computerize solid passwords and rotation of secret wording will protect from digital assault ([6]. Both authors mentioned that hackers can hack by sending an email that looks real. So, the users won't be aware of the upcoming virus. Besides that, the hackers can utilize your login data to remotely get too touchy information put away on the cloud.

4. MATERIALS

Material for cloud computing hardware may be different depending on workloads that the cloud supports. Data storage is one example of this variation. When a cloud vendor establishes a cloud center for the user, the hardware material may be different from other cloud vendors.

Cloud Data Centers - Cooling Hardware: There are different tools for cooling of hardware, such as computer room air conditioning (CRAC) are provided for cloud data centers for cooling of hardware. Heating, ventilation, air conditioning (HVAC) is also another hardware for cooling and is inbuilt. Computer room air handler (CRAH), it uses fans and chilled water coils to remove the heat. As the hardware produces tremendous heat, it is required to be cooled.

CPU, Memory, and Local Disk Equipment in Cloud Computing Centres: Conventional information will in general be uploaded with an agreement of additional resources, such as central processing units, plates, and memory. Plates absorb the heat and the room is cooled. The server supports the data in the cloud by self-benefit provisioning to adjust the limits according to the requirement.

Data Storage and Networking in cloud Data Centres:

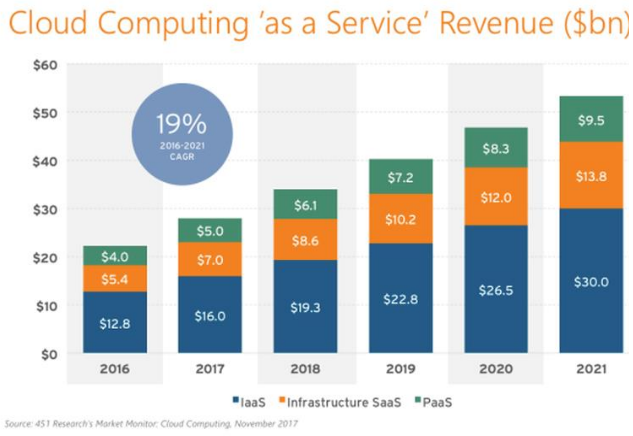
Data storage and managed collectively if they're going to be productive. This issue has complicated the manner in which the data centers have been overseen and has forced associations to purchase a great deal of extra equipment and programming. The cloud data center can be built to overcome this issue. The cloud knows where its information should be so that it is so proficient in the manner in which it oversees outstanding tasks at hand. It's really designed to oversee information productively.

Redundancy in Data Center Hardware

Data centers should always move information around the system for backup and disaster recovery. Data centers support such a significant number of various remaining tasks that have numerous ways to deal with reinforcement and recuperation must be taken. This makes data complicated and expensive by backing up and recovering data. It is designed to handle data consistently in contrast with the cloud.

Software Embedded within the Data Center

In discussion with the applications, however, a lot of programming is connected at a systems level. This sort of system-level programming is a major expense due to loads of work with many software elements in various operating systems in the traditional data center. Cloud computing utilizes an abstraction layer that virtualizes assets and logically exhibits them to users through application program interfaces and API-enabled command-line or graphical interfaces. These virtualized assets are facilitated by a service provider or IT division and are conveyed to users over the internet. These assets incorporate virtual machines and components, such as servers, firewalls, load balancers and storage capacity.



Source: 451 Research's Market Monitor: Cloud Computing, November 2017

Fig (3). Revenue

According to the result of research conducted shows the number of usages in cloud computing is increasing at a faster rate than analysts expected every year, global spending on cloud service will reach $260bn this year up from $219bn. we can see that is about one-third of information technology enterprise spending will be on cloud service this year that indicating a development dependence on outside providers of information regarding infrastructure, application, and security services. Cloud service providers are specializing in running and securing these services will have better skills and experienced workers than a small business affords to hire, cloud computing able to deliver a secure and efficient service to consumers.

5. CONCLUSIONS

Cloud computing is the innovation process of this and the upcoming generation. Analysis of data and information is the most important task for any organization for decision making there for reducing the cost is mandatory. The service provider and consumer should assure privacy and security, then any of the organizations can take the risk to transfer their data or information into the cloud. In this paper, the security and privacy of cloud computing that is currently faced are highlighted. Cloud computing can possibly turn into an advancing protected, virtual, and economically viable Information Technology solution later on. We endeavored to understand numerous issue and solve with our solution. In the future, data security and privacy should be created in such a way where a user that uses it can access it without any hesitation when sharing their data.

6. REFERENCES

[1] Sotto LJ, Treacy BC, McLellan ML. Privacy and data security risks in cloud computing. Electronic Commerce &amp; Law Report2010, 15 ECLR 186.

[2] Sajithabanu S, Dr Prakash Raj. George E "Data Storage Security in Cloud" *InternatIonal Journal of Computer ScienCe and technology*, **2**(4), (2011).

[3] Dinh HT, Lee C, Niyato D, Wang P "A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches" . *Wirel Commun Mob Comput* **13**: 1587-1611, (2013)

[4] Fernando N, Loke SW, Rahayu W "Mobile Cloud Computing: A Survey", *Future Genereration Computer Systems*, **29**: 84-106, (2013)

[5] K. Benson, R. Dowsley, and H. Shacham, "Do you know where your cloud files are?" in Proceedings of the 3rd ACMworkshop on Cloud computing security workshop, pp. 73–82, ACM, October 2011.

[6] S. Pearson and A. Benameur, "Privacy, security and trust issues arising from cloud computing," *in Proceedings of the 2nd IEEE International Conference on Cloud Computing Technology and Science (CloudCom '10)*, 693–702, IEEE, (2010).

[7] A. Squicciarini, S. Sundareswaran, and D. Lin, "Preventing information leakage fromindexing in the cloud," *in Proceedings of the 3rd IEEE International Conference on Cloud Computing (CLOUD '10)*, 188–195, (2010).

[8] R. Arora, A. Parashar, and C. C. I. "Transforming, Secure user data in cloud computing using encryption algorithms*,"* *International Journal of Engineering Research and Applications*, **3**(4), 1922–1926, (2013).

[9] Inayat, I., Salim, S. S., & Kasirun, Z. M., "Socio-technical aspects of requirements-driven collaboration (RDC) in agile software development methods". *Proceedings of International Conference on Open Systems*, IEEE, (2012).

[10] Kalem, S., Donko, D., & Boskovic, D., "Agile Methods for Cloud Computing". *Proceedings of 36th International Convention on Information & Communication Technology Electronics & Microelectronics (MIPRO)* IEEE, (2013).

[11] Xianfeng, L., Kun, T., & Xiu, X., "Technology base and management pattern of agile product development", *In proceedings of 4th International Conference on Wireless Communications, Networking and Mobile Computing*, IEEE, (2008).

[*] For correspondence; Tel. + (60) 03-6145 1777, E-mail: leelavathiraj@segi.edu.my