International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Security-Related Hidden Issues and Challenges of Cloud Computing In the 4.0 Era

Nguyen Tan Danh

FPT University, Vietnam
Corresponding author E-mail: nguyentandanh0774@gmail.com

ABSTRACT

The security problem of cloud computing comes in the form of data leaks or related to access control. No matter what happens, care needs to be taken when choosing software or solutions. Businesses need to address these security challenges. At the same time, provide individual solutions for vulnerabilities discovered when using cloud computing technology, to meet business challenges and customer needs. Cloud computing is a matter of great concern in the technology world. This article studies security, safety, as well as deploying cloud computing technology for organizations and businesses. Based on current research documents, the results show that protecting cloud computing has many challenges and managers need to anticipate possible risks to avoid unexpected incidents in the future.

Keywords: cloud computing, risk, challenge, data

1.Introduction

Some companies claim that they have difficulty dealing with data breaches, perhaps because they are too small to respond to cyber attacks, or because they are too large to fully protect themselves. However, software as a service (SaaS) and other breaches are increasing every year, regardless of company size, industry or operating system (Takabi et al., 2010).

To prevent loopholes, companies can implement a variety of cybersecurity measures, train employees on data security, retain only the information that is absolutely necessary for the business, and follow up-to-date procedures. strict security. These are common practices of platform as a service (PaaS).

The strong development of cloud computing has attracted many scientists, universities and information technology (IT) companies to invest in research. Many experts and organizations have given their definition of cloud computing. According to statistics of "Cloud Magazine", there are currently more than 200 different definitions of cloud computing. Each research group gives the definition according to its own understanding and approach, so it is difficult to find a most general definition of cloud computing. Here are some definitions of cloud computing (Moura & Hutchison, 2016).

More and more companies are involved in the development of cloud computing applications, typically Microsoft, Google, Intel, IBM, etc. That has created a large market for applications. Cloud computing, bringing more choices to individuals and organizations wishing to "cloud" their applications and data. According to experts, the development of cloud computing in the future will focus on 3 main issues, including: Federated ability, automation (Automated) and device recognition end (Client aware). These are also new approaches to information technology automation, allowing to meet user requirements in a new, more efficient and cost-effective way. Federated clouds will allow for faster sorting of resources, while endpoint-aware clouds will utilize the unique features of each device in an optimal way (Takabi et al., 2010).

2.Some security challenges when relying on cloud computing for business

2.1 Data breach

Some companies claim that they have difficulty dealing with data breaches, perhaps because they are too small to respond to cyber attacks, or because they are too large to fully protect themselves. whole. However, software as a service (SaaS) and other breaches are increasing every year, regardless of company size, industry or operating system (Moura & Hutchison, 2016).

To prevent loopholes, companies can implement a variety of cybersecurity measures, train employees on data security, retain only the information that is absolutely necessary for the business, and follow up-to-date procedures. strict security. These are common practices of platform as a service (PaaS).

2.2 Access Control

When cyber attackers have valid system access, even the most advanced cloud computing systems cannot protect themselves from attacks and exploits. Unauthorized access is a big problem, regardless of industry or size, unauthorized access is a very common practice (Hoi, 2019).

To control and manage access behavior, companies should use security measures such as multi-factor authentication, single-use OTP passwords. This can reduce the amount of unauthorized access and better manage data theft threats in the data center (Moura & Hutchison, 2016).

2.3 Data loss

Data loss is usually an internal business problem, not a cyberattacker's problem. Regardless of the accident, human error is the most important factor. If proper safeguards are not taken, data may be lost forever (Rao & Selvamani, 2015).

As a precaution, customers using cloud computing services should review the contract terms of data loss and understand who is responsible in the event of data loss. Many cloud service providers include data backup as part of their agreements (Takabi et al., 2010).

2.4 Denial of service

Denial of Service (DoS) attacks render an enterprise's computing power, systems, or networks inoperable. Cyber attackers can even pay other attackers to take control and implement denial of service. Some might blame these cyberattacks on the rise of cryptocurrencies, rather than cloud computing infrastructure (Rao & Selvamani, 2015).

The key to protecting cloud systems and services from denial of service (DoS) attacks is to build redundancy in the infrastructure. Companies can then configure the network specifically for denial of service (DoS) attacks through hardware and software. Finally, DNS servers must be protected to prevent the company's Web server from disrupting operations.

Security is one of the most concerned issues of businesses and individuals using cloud computing services. Data breaches and cyberattacks continue to remind people of the importance of security. While some companies may not be able to implement protections on their own, they can get the help of a third party (Akin et al., 2014).

Although large companies have more secure cloud services, they also have to pay high costs. On the other hand, many small and medium enterprises are at risk due to lack of experience. As a result, companies need to expand their resources, budgets, and skills so they can better conduct their business while deploying security solutions (Attaran et al., 2017).

3. Some service models of cloud computing

Cloud Computing has 4 service models including Public Cloud, these are services on the Cloud Computing platform for individuals and organizations to rent and share resources. The second is Private Cloud, this type is used within a business and is not shared with users outside that business. The third is Hybrid Cloud, this is a hybrid model (hybrid) between Public Cloud and Private Cloud models. Fourth is Community Cloud. This is a service on Cloud computing platform that companies jointly build and provide services to the community (Attaran et al., 2017).

Public Cloud are services provided by 3rd parties (sellers). They exist outside of corporate firewalls and are managed by the cloud provider. It is built for public use, users will register with the provider and pay a usage fee based on the provider's pricing policy. Public cloud is the most commonly used deployment model of cloud computing today.

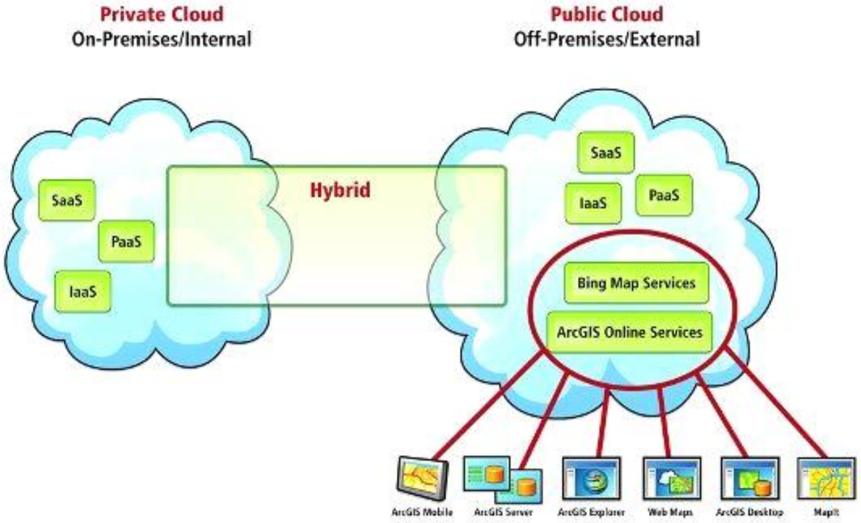

Figure 1. The model of Public Cloud

Public Cloud has one obstacle, which is the loss of control over data and data security issues. In this model, all data is on the Cloud service, protected and managed by that Cloud service provider. This makes customers, especially large companies, feel unsafe for their important data when using Cloud services (Figure 1).

Whereas, Private Cloud are cloud computing services provided in enterprises. These “clouds” exist inside corporate firewalls and are directly managed by businesses. This is an inevitable trend for businesses to optimize information technology infrastructure (Subramanian & Jeyaraj, 2018).

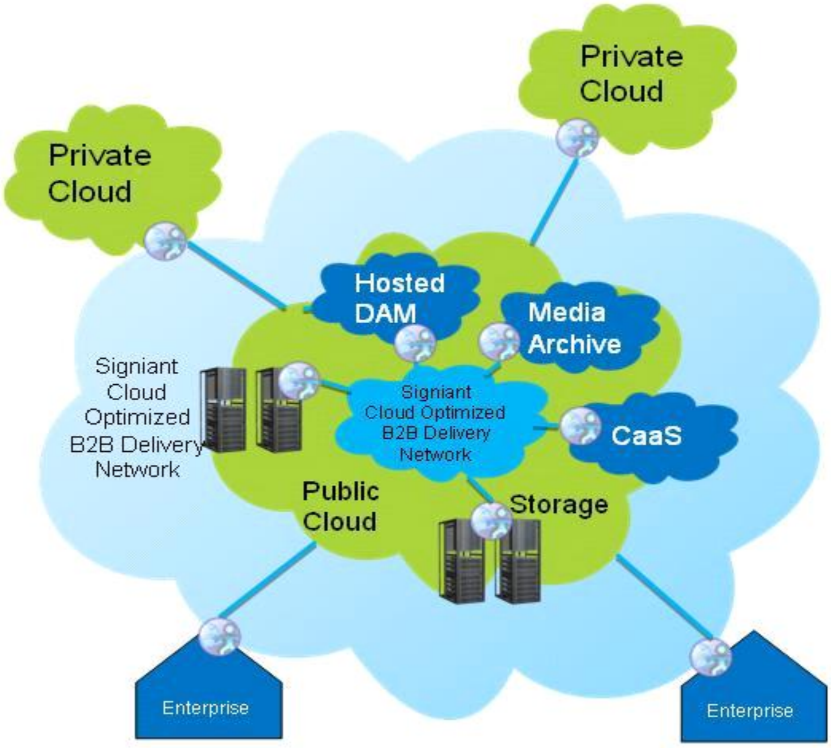

Figure 2. The model of Hybrid Cloud

Playing an important role is Hybrid Cloud, which is a combination of private cloud and public cloud. Allows us to exploit the strengths of each model as well as provide the optimal usage method for users. These “clouds” are typically created by the enterprise, and management is split between the enterprise and the public cloud provider (Figure 2).

4.Some advantages and disadvantages when deploying cloud computing

Firstly, according to the traditional model, in order to have infrastructure, machines and human resources, users need time and money to build plans, invest in infrastructure, invest in machinery and people. Administration, etc. This cost is not small and sometimes it is not used effectively, for example, not meeting enough or not using full capacity after being put into use, etc. Difficulties This will be solved in the cloud computing model, with the motto "pay as you use" (users only pay for what they used).

Secondly, the processing speed is fast, no longer depending on the device and geographical location, this allows users to access and use the system through a web browser anywhere and on any device. which they use (such as a PC or a mobile device, etc.).

Thirdly, it is easy to expand and upgrade, instead of having to invest in new or upgrade hardware, software, management team, etc. to expand or upgrade the system, with cloud computing, users just send the request to the service provider (Subramanian & Jeyaraj, 2018).

However, there are certain obstacles that cannot be avoided. The first is privacy. Information about users and data stored in the cloud is not guaranteed to be private, and such information may also be used for other purposes (Akin et al., 2014).

The second is availability, cloud computing centers or network infrastructure may have problems, causing cloud services to "hang" unexpectedly, so users cannot access services and data. themselves during certain periods of time (Rong et al., 2013).

Next is the risk related to the possibility of data loss. Some online data storage services in the cloud suddenly stop working or do not continue to provide services, even in some cases, for some reason, user data is lost and cannot be accessed. recoverable.

Finally, there is security. The problem of centralizing data on "clouds" is an effective way to increase security, but on the other hand is also a concern of cloud computing service users, because once the clouds are attack or break in, all data will be taken over.

5. Cloud computing classification

Basically, cloud computing can be classified as Public Cloud. Public cloud applications, storage, and other resources are made available to the public by an available service provider. These services are free or pay-per-use. Generally, the user's data in the public cloud will be stored in the cloud and delegated to the service provider for management (Attaran et al., 2017).

Next comes the Private Cloud, which is a cloud computing infrastructure that only works for a single organization, whether managed, hosted internally (internally) or by a third party (external). With a private cloud, users will be assured of higher data security, which is suitable for users with sensitive data and requires high privacy (Subramanian & Jeyaraj, 2018).

Next is Hybrid Cloud, which is a composition of two or more clouds (private cloud and public cloud) that keep the same entities but link them together, providing the benefits of multiple models deployment form. Using a “hybrid cloud” architecture, companies and individuals can handle failures, combined with immediate on-premises usability, without depending on an internet connection.

6. Data safety and security in cloud computing

Ensuring security is vital to the development of cloud computing in practice. Currently, many organizations and businesses have researched and offered many secure solutions for cloud computing (Kuyoro et al., 2011).

Encryption/decryption and authentication are done through Encryption Proxy. This model ensures safe and confidential data during transmission and storage between users and the cloud. In order for ciphertexts to still be processed and stored without needing to be decrypted, homomorphic encryption algorithm and fully homomorphic data encryption algorithm are being studied and applied in this model (Subramanian & Jeyaraj, 2018). Confidential information of users for encryption/decryption is stored in Secure Storage.

VPN technology in traditional network systems has promoted many advantages and is quite popularly used. However, with cloud computing technology that always requires flexibility (dynamic) and flexibility (elastic) in organization and system management, dynamic VPN or elastic VPN techniques will be suitable. When the number of VPN connections in the cloud computing system is large, the corresponding VPN setup model will be required. There are two VPN models that are often of interest: Hub - and - Spoke and Full- Mesh.

7. Development trend of cloud computing

Recently, besides providing cloud computing models and services for enterprises, vendors are making efforts to introduce their cloud solutions and services to administrative authorities. state for developing countries. Popular cloud services such as Amazon's EC2, Microsoft's Azure, IBM's Smart Cloud Enterprise, Google's App Engine, Redhat's Redhat's Openshift, Vmware's Cloud Foundry, Digital Content and Software Industry Institute Vietnam has iDragon Clouds, etc.

In which Google Cloud, Redhat's Openshift, Vmware Cloud Foundry and NISCI iDragon Clouds are open source PaaS, allowing execution on a low-cost and easy-to-replace infrastructure. According to many experts, the number of people using the public cloud will reach 1 billion by 2020. It is said that in 2012 around the world, there are about 1 billion people using traditional systems such as Microsoft Office, OpenOffice or LibreOffice, Microsoft Exchange or Sharepoint, IBM Lotus Notes, by 2020 everyone will move to the public cloud. The International Data Corporation (IDC) has published a new study showing that many large firms in the technology industry will find it difficult to maintain their current position, and may even disappear in the market if they cannot adapt to the new environment. cloud trends. IDC experts have commented: Big companies are all facing a big shift. Hewlett-Packard is an example. Microsoft, Intel, SAP, RIM, Oracle, Cisco, Dell are also having to change if they want to survive and at least a third of them will die around 2020 before the advancement of Amazon, Google, Salesforce.com, or VMware, etc. That forces technology companies that provide traditional software to become cloud computing service providers.

8. Conclusion

Although it has only been developed for a short time. However, today's cloud computing has been very popular application. Cloud computing technology model (Cloud Computing) and practical applications are always important in applying to realize the goals set out by individuals and businesses throughout the operation process. Once you have put the data on the cloud storage system, it will be very easy for managers to control and manage the data of their entire company. Most of the platforms used for data analysis today are capable of handling structured or unstructured data with integrity.

References

- Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy*, *8*(6), 24-31.
- Subramanian, N., & Jeyaraj, A. (2018). Recent security challenges in cloud computing. *Computers & Electrical Engineering*, *71*, 28-42.

- Moura, J., & Hutchison, D. (2016). Review and analysis of networking challenges in cloud computing. *Journal of Network and Computer Applications*, *60*, 113-129.
- Rong, C., Nguyen, S. T., & Jaatun, M. G. (2013). Beyond lightning: A survey on security challenges in cloud computing. *Computers & Electrical Engineering*, *39*(1), 47-54.
- Attaran, M., Attaran, S., & Celik, B. G. (2017). Promises and challenges of cloud computing in higher education: a practical guide for implementation. *Journal of Higher Education Theory and Practice*, *17*(6), 20-38.
- Hoi, H. T. (2019). Efficiency of Japanese-Vietnamese Translation Job Thanks to the Use of Technology in the Fourth Industrial Revolution. In *Proceedings of the 2019 The 3rd International Conference on Digital Technology in Education*, 181-184.
- Rao, R. V., & Selvamani, K. (2015). Data security challenges and its solutions in cloud computing. *Procedia Computer Science*, *48*, 204-209.
- Akin, O. C., Matthew, F., & Comfort, D. (2014). The impact and challenges of cloud computing adoption on public universities in Southwestern Nigeria. *International Journal of Advanced Computer Science and Applications (IJACSA)*, *5*(8), 13-19.
- Kuyoro, S. O., Ibikunle, F., & Awodele, O. (2011). Cloud computing security issues and challenges. *International Journal of Computer Networks (IJCN), 3*(5), 247-255.