Al-Farouk journal of sciences
Volume (2), Issue (1) (March, 2026)
ISSN: 3135-2359

مجلة الفاروق للعلوم
المجلد (2) العدد 1 مارس 2026
ردمد: 3135-2359

Personal Data Security and Protection Solution Proposals in Cloud Computing

Tarek Mosbah Abdala

Department of Professions Computer

Higher Institute For Comprehensive Profession Kabaw

tarekmosbah2014@gmail.com

تاريخ الاستلام: 2026/01/08 تاريخ المراجعة 17 / 2 / 2026 تاريخ القبول: 2026/03/10- تاريخ النشر: 17/ 03/ 2026

الملخص

الحوسبة السحابية من أكثر المصطلحات شيوعًا في صناعة الحواسيب حاليًا .تُمكّن المحاكاة الافتراضية من مشاركة الموارد، بما في ذلك البرامج والمنصات والبنية التحتية .وتُعدّ المحاكاة الافتراضية التقنية الأساسية التي تقوم عليها مشاركة موارد الحوسبة السحابية .يطمح هذا النظام إلى أن يكون ديناميكيًا وموثوقًا وقابلًا للتخصيص، مع مستوى عالٍ من ضمان الخدمة . يُعدّ الأمن بنفس القدر من الأهمية في الحوسبة السحابية كما هو الحال في أي مكان آخر .لدى الكثيرين وجهات نظر مختلفة حول الحوسبة السحابية .يرى البعض أن استخدام الحوسبة السحابية محفوف بالمخاطر يبذل مزودو خدمات الحوسبة السحابية جهودًا كبيرة لضمان الأمن .تتناول هذه الدراسة بعض الثغرات الأمنية الهامة في الحوسبة السحابية، بالإضافة إلى الحلول المتاحة لتلك المشكلات الأمنية في قطاع الحوسبة السحابية.

الكلمات المفتاحية: الحوسبة السحابية، نماذج خدمات الحوسبة السحابية، الأمن، التهديدات، وسائل الدفاع المحتملة.

ABSTRACT

Cloud computing is one of the most popular terms in the computer industry right now. Virtualization enables resource sharing, which includes software, platform, and infrastructure. The underlying technology underpinning cloud resource sharing is virtualization. This environment aspires to be dynamic, dependable, and configurable, with a high level of service assurance. Security is just as important in the cloud as it is everywhere else. Various people have different perspectives on cloud computing. Some people feel that using the cloud is risky. Cloud providers go to great lengths to assure security. This study looks at a few important security vulnerabilities with cloud computing, as well as available remedies to those security issues in the cloud computing sector.

Keywords: Cloud Computing, Cloud Computing Services Models, Security, Threats, Potential Defenses.

1- INTRODUCTION

Cloud computing is services that are provided to customers through a network on a leasehold basis with the ability to expand up or down their service requirements. Usually be delivered cloud computing services by a third party provider who owns the infrastructure. Advantages but not limited to include scalability, flexibility and efficiency [1]. Cloud computing allows business model for organizations to adopt IT services without investing in advance. Despite the potential gains from cloud computing, organizations slow to accept for reasons of security and the challenges associated with it. Security is the most concerned issues that hinder the growth of the cloud.

Cloud computing can be considered new computing model that affect the availability of greater flexibility and at a lower cost. Because of this, cloud computing received a great deal of attention lately. Cloud computing services to take advantage of economies of scale achieved through the use of diverse resources, specialization, and other efficiencies. However, it is a new form of distributed computing is still in its infancy. And often used the term itself today with a range of meanings and interpretations. Three models have evolved service referred to widely

Cloud computing is a way of IT delivery, which provides users with their demands to access to combine the flexibility and wide-ranging, from cloud computing assets content of services and applications, servers, networks, and storage facilities.

2- WHAT IS CLOUD COMPUTING

.Cloud computing is computing model, where they are connecting a wide range of networking systems in the private or public sector, to provide the infrastructure for data vital and viable and store files. With the advent of this technology, the cost is reduced expense, application hosting and content storage and delivery significantly.

The ideas of cloud computing on a very basic principle of “re-use of information technology capabilities. Difference is that cloud computing brings compared to traditional concepts of grid computing, distributed computing, utility computing, or autonomic computing is expanding horizons across organizational boundaries.

It can also be defined as “management of resources, applications and information as services over the cloud (internet) on demand”.

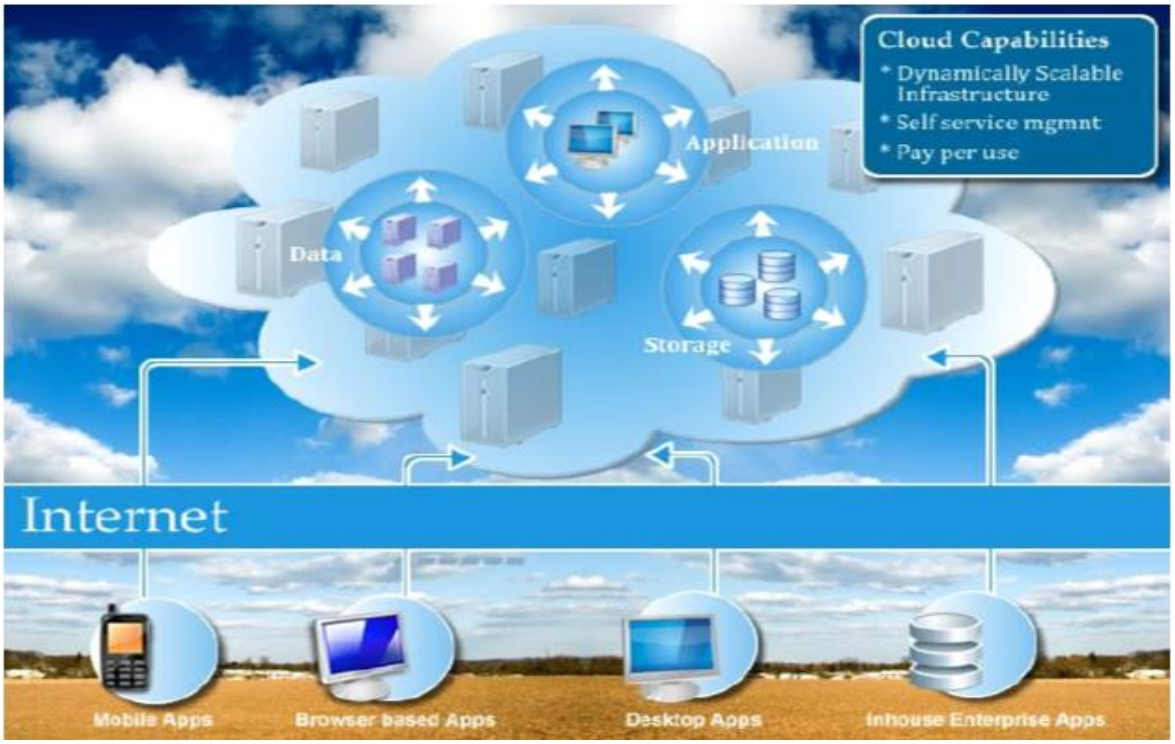

Figure 1: Components of the K

3- TYPES OF CLOUD

Different clouds for different needs:

1- Public cloud

Public cloud it is very popular in cloud computing, by participating equipment, public cloud present the greatest possible cost-effectiveness, present also greatest scalability and flexibility.

Although, public cloud does not have the same regulatory scrutiny, it can be a security concern through Access the shared Internet connections. This fact makes public cloud is less than ideal to host applications and sensitive data.

2- Private cloud

To increase security, many companies looking for more private and secure cloud solution. In a private cloud, and devote a lot of resources in the operating environment for a single client, and to ensure that customer data and never share the virtual space with another company. With a private entrance to replace leased lines and Internet connections, and can also give the customer access to security controls and management as needed.

3- Hybrid cloud

Some companies manage some resources inside their cloud while other functions are managed externally. For example, a company might choose to send their investment accounting function to the cloud, while other tasks put it within their own cloud.

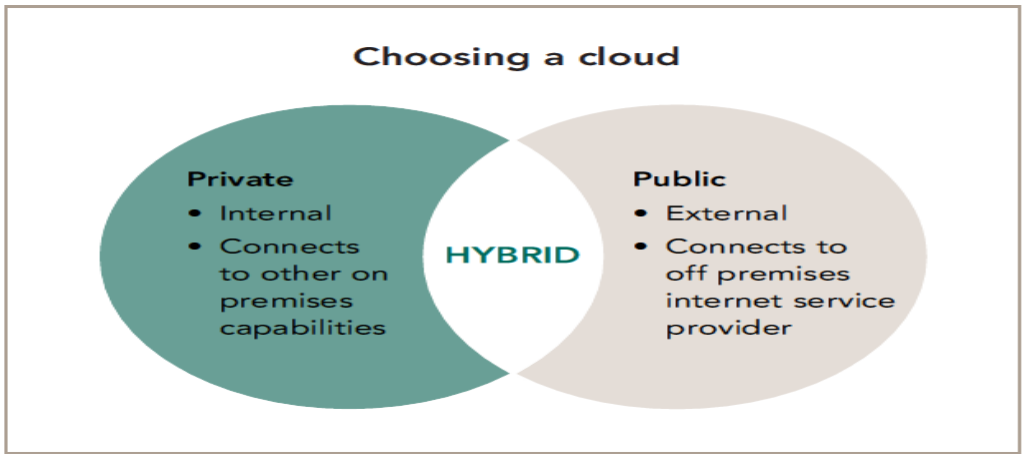

Figure 1: Components of the Kjeldahl apparatus.

4- Cloud Computing Services Models

1. Service Models

Three types of models exist for providing services of cloud. These three models are often referred to as the "SPI Model (Software, Platform and Infrastructure)[2].

• Software as a Service (SaaS): Customers obtain the facility to access and use an application or service that is hosted in the cloud. where necessary information for the interaction between the consumer and the service is hosted as part of the service in the cloud.

• Platform as a Service (PaaS): Customers obtain access to the platforms by enabling them to organize their own software and applications in the cloud.

• Infrastructure as a Service (IaaS): The facility provided to the customer is to lease processing, storage, and other fundamental computing resources. The customer not manage or control the basic cloud infrastructure but has control over operating systems, storage, deployed applications.

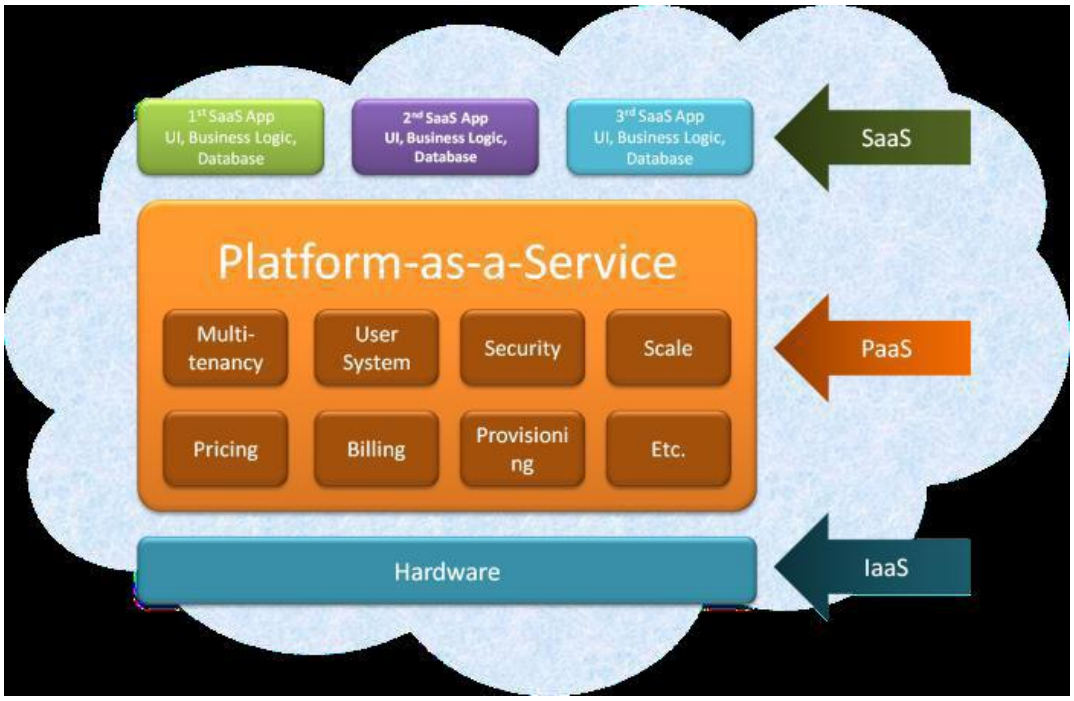

Figure 1: Cloud Computing Services Models

5- Security Issues In Cloud Computing

Cloud computing is a model for information and services by using existing technologies. It uses the internet infrastructure to allow communication between client side and server side services/applications[2].

Cloud service providers (CSP's) exist between clients that offers cloud platforms for their customers to use and create their own web services.

When making decisions to adopt cloud services, privacy or security has always been a major issue. To deal with these issues, the cloud provider must build up sufficient controls to provide such level of security than the organization would have if the cloud were not used[3].

Our research focus is to provide a solution for the threats that are the major issue for anyone when they want to adopt cloud services for their work. For this purpose, a framework should be designed for execution of data and information securely in cloud environment. It will protect users' data, messages, information against various attacks. Some of the most common assets are described in Table.

Assets	Threats
Data Loss or Leakage	Loss of data , attack the security ,the intellectual property could have competitive and financial implications. or , may be doing some violation .
Applications/Functions/Process	Emerged in recent years over attacks on a common IT environments within cloud computing.
	Criminals influence of new technologies to address the information and avoid detection.

Table 1.1: Assets and Threats for cloud computing

6- SECURITY REVIEW

➢ **Identify the asset(s) for cloud computing**

- Data Loss or Leakage
- Applications/Functions/Process

Assets	Threats	Potential Defenses
Data Loss or Leakage	Loss of data , attack the security ,the intellectual property could have competitive and financial implications. or , may be doing some violation .	Implement strong API access controls; Firewalls ,Encryption , Authentication Intrusion Detection Prevention , Systems Virtualized Private Networks , File Integrity Monitoring

Applications/Functions/Process	Emerged in recent years over attacks on a common IT environments within cloud computing.	Implement best security installation and configuration. Choosing a hosting service with extensive, private,
	Criminals influence of new technologies to address the information and avoid detection.	- More stringent for initial registration - more stringent for checking the validation processes. To Comprehensive inspection of customer network traffic and keep an eye for public blacklists .

Table 1.2: **Assets, Threats and Potential Defenses for cloud computing**

7. CONCLUSION

There are many new technologies emerging at a rapid rate, and each technological progress and with the possibility to make human life easier. However, we must be very careful to understand the risks and security challenges in the use of these techniques. Cloud computing is no exception. In this debate and highlights the security considerations and the major challenges currently facing in cloud computing. Cloud computing has the potential to become the frontrunner in promoting safe and economically viable and virtual IT solution in the future.

8. REFERENCES

1. Abdul-Jabbar, S.S., Aldujaili, A., Mohammed, S.G. and Saeed, H.S., 2020. Integrity and Security in Cloud Computing Environment: A Review. Journal of Southwest Jiaotong University, 55(1).
2. Alam, T., 2020. Cloud Computing and its role in the Information Technology. IAIC Transactions on Sustainable Digital Innovation (ITSDI), 1(2), pp.108-115.

3. 28. Zhang, D., Jiang, T. and Wu, S., 2020. Brief Talk on Cloud Computing Technology. International Journal of Social Science and Education Research, 3(6), pp.168-171.

1. Tadapaneni, N. R. (2020). Cloud Computing - An Emerging Technology. International Journal of Innovative Science and Research Technology. 5.

2. Jamil, D., Zaki, H. (2011) Cloud Computing Security. International Journal of Engineering Science and Technology 3(4), 3478–3483.

3. Tadapaneni, N. R. (2017). Different Types of Cloud Service Models. Available at SSRN 3614630.

4. Bikram, B. (2009) Safe on the Cloud. A Perspective into the Security Concerns of Cloud Computing 4, 34–35.

5. Dikaiakos, M.D., Katsaros, D., Mehra, P. (2009) Cloud Computing: Distributed Internet Computing for IT and Scientific Research 13, 10–13.

6. Tadapaneni, N. R. (2018). Cloud Computing: Opportunities and Challenges. SSRN Electronic Journal. 10.2139/ssrn.3563342.

7. Srinivas, Reddy, Qyser, J. (2014), Cloud Computing Basics, Build. Infrastructure. Cloud Security., vol. 1, pp. 3–22,

8. Ion, I., Sachdeva, Kumaraguru, P., & Čapkun, S. (2011). Home is safer than the cloud: privacy concerns for consumer cloud storage. In Proceedings of the Seventh Symposium on Usable Privacy and Security (p. 13).

9. 10) Puthal, Sahoo, Mishra, Swain, P.(2015) cloud computing features,Issues and Challenges:A big picture", International Conference on Computational Intelligence & Networks, pp. 116-123.

10. Tadapaneni, N. R. (2020). Artificial Intelligence Security and Its Countermeasures. International Journal of Advanced Research in Computer Science & Technology, Vol. 8.

11. Tadapaneni, N. R. (2020). A Survey Of Various Load Balancing Algorithms In Cloud Computing. International Journal for Science and Advance Research in Technology, 6.

12. Selviandro, Suryani, A. Hasibuan, S.(2015), Open learning optimization based on cloud technology: case study implementation in personalization E-learning, February 16~19, pp. 541-546.

13. Winkler, V.(2011) Securing the Cloud, Cloud Comput. Secur. Tech. tactics. Elsevier.

14. Sabahi, F.(2011). Virtualization-level security in cloud computing, 2011 IEEE 3rd Int. Conf. Communication. Software. Networks, pp. 250–254