A Review of Emerging Security Issues In Cloud Computing

[1]Roselyne Akinyi Oluoch [2]Nelson Masese

Department of Computer Science and IT, Kabarak University
P. O. Private Bag - 20157 Kabarak, Kenya

Abstract: *The rapid growth of technology adaptation has consequently led to the growth of new ways of delivering technology to business organizations; one of them is through cloud computing. It is a technology that enables instant, on-demand access to a shared pool of computing resources delivered with minimal customer management. Its key characteristics are on-demand self-service, rapid elasticity, measured service, resource pooling, and network access. Customers, therefore, spend less to access computing services at any time with any device. However, this is challenged by security issues present. This paper is a review of cloud computing service delivery models and some of the security challenges surrounding each model. Some potential countermeasures to the security challenges include: encryption, intrusion tolerant systems, authentication and authorization systems, disaster recovery systems, trusted third-party, virtual machine isolation and strong security policies. This study recommends that security be treated as a shared responsibility between the organization's IT department and CSP.*

Keywords: *Cloud computing, Security issues, Service delivery models, Deployment models, Countermeasures*

I. INTRODUCTION

For several years, many organizations have been using technology to carry out business transactions and routine business management processes due to its efficiency and effectiveness. However, the rate of adoption of technology in managing business organizations has increased exponentially in the last decade due to growth in the size of business activities, competition, and continued globalization [1]. This has prompted the continuous development of innovative ways of delivering technology to handle rising complex business transactions [2]. One of the latest innovations in the field of technology is cloud computing [3], [4].

Cloud computing is a computing technology that provides an infinite number of computing resources to end-users based on their demands, anywhere and anytime in pay-as-you-go fashion where users pay only for the services they use [5]. The study by [6] defines cloud computing as a technology that enables instant, on-demand access to a shared pool of computing resources that can be delivered with minimal customer management. The features of loud Computing can provide advanced computational characteristics to multi-agent systems [7]. According to [8], [9]; cloud computing has five key characteristics as illustrated in Table I (see Table I):

TABLE I

Key Characteristics Of Cloud Computing

	Cloud characteristic	**Explanation**
i.	On-demand self-service	The users of cloud computing can access computing resources automatically**.** For example, networks, servers, software, and storage devices can be accessed automatically.
ii.	Rapid elasticity	Cloud computing users can scale-up or down-scale the services to suit their individual needs. This enables cloud users to quickly adapt to the changing business environment.
iii.	Measured service	Cloud computing users have the opportunity to use only what is necessary.

		This enables them to operate efficiently since they will only pay for what they have consumed.
iv.	Resource pooling	Cloud computing enables the pooling of different resources to serve multiple customers using a multitenant model. With this feature, organizations will enjoy the low cost of computing due to economies of scale.
v.	Network access	Cloud computing enables users to access computing resources remotely using devices such as desktop computers, laptops, PDAs, and mobile phones.

The five characteristics clearly show that cloud customers do not have to spend vast amounts of capital in order to access computing resources [10]. This provides a level playing field to both small-sized and large-sized organizations; it also enables an organization to start small and successively increases its computing resources. The characteristics also show that customers can access computing resources any time of day or night and that they can access the resources remotely using any device [11].

However, despite the several benefits derived from cloud computing, security issues present the most significant challenge to adopting this model of delivering computing resources [12]–[14]. This paper is a review of cloud computing deployment models, cloud computing service models, and security issues present in a cloud computing environment. The paper also outlines some potential countermeasures to cloud computing security issues.

A. Problem statement

Cloud computing is a technology that promises to increase efficiency and effectiveness in today's organizations. However, this technology has many security issues due to the methods used in service delivery. The security issues present a significant challenge in the adoption of cloud computing services. This study focuses on reviewing existing literature about security issues in cloud computing service delivery models. The study also provides some potential countermeasures to security issues.

B. Objective of the study

The main objective of this study is to review the current literature in cloud computing. The study focuses on emerging security issues in cloud computing service delivery models and provides some potential countermeasures to cloud computing security issues.

II. CLOUD COMPUTING DEPLOYMENT MODELS

In [15]–[17], the authors state that cloud computing deployment models can be classified into:

i. Private cloud - The cloud computing infrastructure is owned by a single organization. It can be managed by the organization itself or a third-party, within the organization's premises or off-site.

ii. Community cloud - The cloud computing infrastructure supports several organizations with similar concerns. It can be managed by the organizations or a third-party, either within the organization's premises or off-site.

iii. Public cloud - The cloud computing infrastructure is owned by a third-party [1] - cloud service provider (CSP). The cloud services are made available by the CSP to the general public.

iv. Hybrid cloud - The cloud computing infrastructure consists of a combination of two or more deployment models. For example, a section of the infrastructure can be dedicated to a single organization, whereas, the remaining section can be shared with other organizations (i.e., community or public clouds)

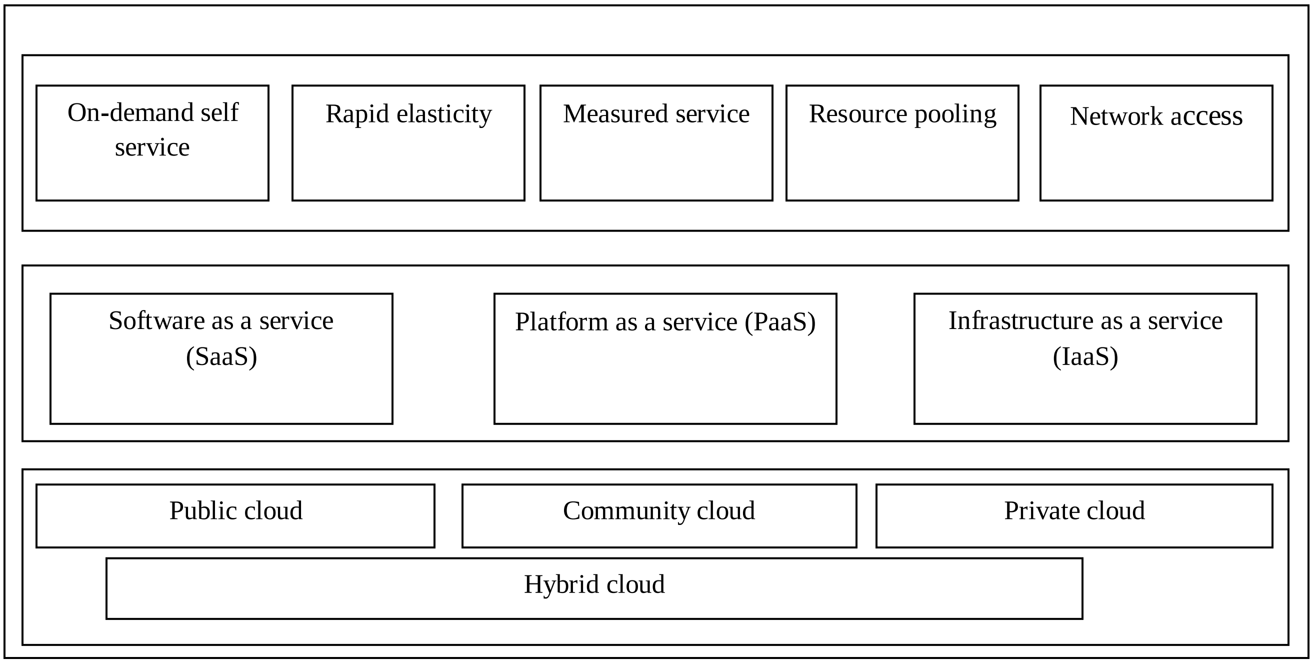

Figure 1: Cloud computing model

The type and level of security to be implemented depends significantly on the deployment model. For instance, a private cloud, particularly one that is solely managed by the organization itself can be considered safer than the community and public clouds. A private cloud provides some form of perimeter security since only members of the organization can interact with the cloud infrastructure. Therefore, unauthorized access can be easily minimized. Public cloud, on the other hand, presents very complex security issues, such as breach of security by employees of CSP, network access issues, and issues related with the shared infrastructure like shared memory, processor, and network [13], [18].

III. CLOUD COMPUTING SERVICE MODELS

According to [19]–[21], cloud computing can be broadly categorized into three service models namely:

i. Software as a Service (SaaS) - This model enables cloud users to access application programs directly from cloud service providers. SaaS is the most popular category of cloud service models. Examples of SaaS include; web-based email services such as Gmail and yahoo; social networking services such as YouTube and Facebook; online gaming services such as Zynga; and others that offer services for business management such as word processors, and electronic calendars [22].

ii. Platform as a Service (PaaS) - This model enables cloud users to deploy their own applications and services. It aims at providing a platform for managing the entire system development life cycle – planning, design, coding, testing, deployment, and maintenance. Cloud users are able to access tools used in an integrated development environment (IDE), making it easy to develop and execute user programs. For example, database management systems (DBMS) [23].

iii. Infrastructure as a Service (IaaS) - This model enables cloud users to access computing resources such as disk drives, processors, servers, and networks. According to [18], IaaS provides the foundation for all cloud services. PaaS builds upon IaaS, and SaaS builds upon PaaS.

IV. CLOUD COMPUTING SECURITY ISSUES

Information systems security aims at achieving three main objectives – confidentiality, integrity, and availability (CIA). Confidentiality is the protection of data from unauthorized access, integrity is the protection of information from modification or deletion, and availability is ensuring that information and other IT resources are made available to legitimate users at the right time [24]. However, the nature of cloud computing services makes them vulnerable to attacks that compromise the three security objectives [25], [26].

A. Security issues with software as a service (SaaS)

SaaS refers to a model that enables users to access applications via the internet. This characteristic of cloud computing environment presents several security challenges including:

i. Eliminates the traditional perimeter that provided some level of protection to the organization's applications. Consequently, any security vulnerability in traditional Web applications is automatically inherited by these online applications [27].
ii. Data access security – Since the CSP and the customer are located in different places, data in transit will be vulnerable to threats such as session hijacking and eavesdropping.
iii. Datacenter security – Organization's data and applications could be vulnerable to unauthorized access or alteration by employees of CSP.

B. Security issues with platform as a service (PaaS)

PaaS model provides cloud users with the environment to develop application programs. However, this characteristic of cloud computing environment exposes the users to security challenges, including:

i. Application integration – Cloud computing users may experience challenges when trying to integrate applications developed using the PaaS model with other applications.
ii. Vendor lock-in – Cloud computing is still struggling with maturity issues; therefore, policies on migrating from one CSP to another may be lacking. It is also not clear whether, on migrating, the applications and processes will be compatible with the new provider's platform [27].
iii. Complexity in the development process – Cloud computing applications developers go through a very complex process in order to develop secure applications. This is due to the dynamic nature of the cloud computing environment.

C. Security issues with infrastructure as a service (IaaS)

As stated by [19], "IaaS is the foundation layer for other cloud layers. Thus, the absence of any form of security in this layer can affect the other two layers in the cloud computing model". Some common security challenges presented at this layer include:

i. Multi-tenancy – Since several different customers' resources reside on the same cloud service provider's resources (memory, processor, and network); issues such as unauthorized access and misuse of resources may arise.
ii. Hypervisor security – Since hypervisors are programs used to provide hardware virtualization and enable multiple operating systems to concurrently execute on one host machine, a compromise on the hypervisor will lead to massive damage due to its effect on the guest machines.
iii. Virtual machine security – Providing consistent security and audits to the virtual machine may prove to be a challenge [23].
iv. Denial of service (DoS) attacks – Security compromise on the vendor's resources may lead to service unavailability to cloud computing customers [24].

V. COUNTERMEASURES TO CLOUD COMPUTING SECURITY ISSUES

The following security techniques ought to be implemented in a cloud computing environment: [14], [28], [29]

i. Encryption – Encryption is a mechanism that converts data into unreadable format. Both cloud computing customers and CSP should encrypt data at rest, data being processed and data in transit [30].
ii. Trusted third party (TTP) – This is an entity that is required to facilitate interactions between two parties (cloud customer and CSP) that both trust the third party [31].
iii. Authentication and Authorization – Authentication and authorization systems are used to verify the identity of users of IT resources and to facilitate non-repudiation respectively. Both the organization and CSP should implement these systems [32].
iv. Virtual machines (VMs) isolation – CSP should facilitate isolation of customer data from one another. Cloud tenants should be segmented into isolated entities [23].
v. Training and education – Organizations should employ IT security professionals in the organization's IT department, as well as provide regular training to cloud users. CSP should also train its employees frequently.
vi. Perimeter security - Implementation of firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and intrusion tolerant systems (ITS) in order to

improve robustness in the cloud computing environment [33].

vii. Backup / Disaster Recovery / Business Continuity – Cloud service providers should provide redundant servers, networks, and other IT resources in order to eliminate or minimize downtime.

viii. Strong security policies – Organizations should develop security policies and always review existing policies to stay up-to-date with the changing technology environment.

VI. CONCLUSION

Cloud computing is a model that ensures economy, elasticity, and convenience in IT service delivery. Thus, it is important for individuals and organizations to understand the security issues associated with cloud computing infrastructure. With this understanding, they will be able to implement the right technologies to deal with cloud computing security issues.

Even when IT infrastructure is moved to the cloud, the responsibility for information security cannot be entirely outsourced to CSP. This study recommends that cloud computing security should be treated as a shared responsibility between an organization's IT department and CSP. This can be achieved through defense-in-depth, for example, recruitment of IT security experts, training of staff, and implementation of IT security policies in both organization and CSP.

REFERENCES

[1] R. M. U. Ullah, K. A. Buckley, M. Garvey, and J. Li, "The Challenges of Cloud Computing in Forensic Science," International Journal of Computer Trends and Technology (IJCTT), vol. 67, no. 7, pp. 40–48, 2019.

[2] S. Iqbal, M. L. M. Kiah, N. B. Anuar, B. Daghighi, A. W. A. Wahab, and S. Khan, "Service delivery models of cloud computing: security issues and open challenges," Security and Communication Networks, vol. 9, no. 17, pp. 4726–4750, 2016.

[3] R. Mahajan1 and D. Singh, "Step by step securing cloud environment," International Journal of General Engineering and Technology (IJGET), vol. 6, no. 4, pp. 47–54, 2017.

[4] K. Wakunuma and R. Masika, "Cloud computing, capabilities and intercultural ethics: Implications for Africa," Telecommunications Policy, vol. 41, pp. 695–707, 2017.

[5] M. Kumar, S. C. Sharma, A. Goel, and S. P. Singh, "A comprehensive survey for scheduling techniques in cloud computing," Journal of Network and Computer Applications, vol. 143, pp. 1–33, Oct. 2019.

[6] V. O. Safonov, Trustworthy Cloud Computing. Hoboken, UNITED STATES: John Wiley & Sons, Incorporated, 2016.

[7] F. De la Prieta, S. Rodríguez-González, P. Chamoso, J. M. Corchado, and J. Bajo, "Survey of agent-based cloud computing applications," Future Generation Computer Systems, vol. 100, pp. 223–236, Nov. 2019.

[8] T. Almarabeh, Y. K. Majdalawi, and H. Mohammad, "Cloud Computing of E-Government," Communications and Network, vol. 8, no. 1, pp. 1–8, Feb. 2016.

[9] T. H. Noora, S. Zeadally, A. Alfazi, and Q. Z. Sheng, "Mobile cloud computing: Challenges and future research directions," Journal of Network and Computer Applications, vol. 115, pp. 70–85, 2018.

[10] N. Subramanian and A. Jeyaraj, "Recent security challenges in cloud computing," Computers and Electrical Engineering, vol. 71, pp. 28–42, 2018.

[11] C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, "Secure integration of IoT and Cloud Computing," Future Generation Computer Systems, vol. 78, pp. 964–975, 2018.

[12] P. Hu, S. Dhelim, H. Ning, and T. Qiu, "Survey on fog computing: architecture, key technologies, applications and open issues," Journal of Network and Computer Applications, vol. 98, pp. 27–42, Nov. 2017.

[13] G. Ramachandra, M. Iftikhar, and F. A. Khan, "A Comprehensive Survey on Security in Cloud Computing," in Procedia Computer Science 110 (2017), 2017, pp. 465–472.

[14] C. Stergiou, K. E. Psannis, B. B. Gupta, and Y. Ishibashi, "Security, privacy & efficiency of sustainable Cloud Computing for Big Data & IoT," Sustainable Computing: Informatics and Systems, vol. 19, pp. 174–184, 2018.

[15] Kh. E. Ali, Sh. A. Mazen, and E. E. Hassanein, "A proposed hybrid model for adopting cloud computing in e-government," Future computing and informatics journal, vol. 3, pp. 286–295, 2018.

[16] P. Kumari and P. Kaur, "A survey of fault tolerance in cloud computing," Journal of King Saud University – Computer and Information Sciences, pp. 1–18, 2018.

[17] B. Varghese and R. Buyya, "Next generation cloud computing: New trends and research directions," Future Generation Computer Systems, vol. 79, pp. 849–861, 2018.

[18] V. Winkler, G. Speake, and P. Foxhoven, Securing the Cloud: Cloud Computer Security Techniques and Tactics. Saint Louis, UNITED STATES: Elsevier Science & Technology Books, 2011.

[19] S. Iqbal, M. L. M. Kiah, N. B. Anuar, B. Daghighi, A. W. A. Wahab, and S. Khan, "Service delivery models of cloud computing: security issues and open challenges," Security and Communication Networks, vol. 9, no. 17, pp. 4726–4750, 2016.

[20] L. Novaisa, J. M. Maqueirab, and Á. Ortiz-Basa, "A systematic literature review of cloud computing use in supply chain integration," Computers & Industrial Engineering, vol. 129, pp. 296–314, 2019.

[21] E. Huey, "Cloud Computing - Challenges and Benefits," International Journal of Computer Trends and Technology (IJCTT), vol. 67, no. 9, pp. 21–24, 2019.

[22] BCS The Chartered Institute for IT, "What is Cloud Computing?," in Cloud Computing: Moving IT out of the office, BCS Learning & Development Limited, 2012, pp. 1–6.

[23] R. P. Padhy, "Cloud Computing: Security Issues and Research Challenges," International Journal of Computer Science and Information Technology, vol. 1, no. 2, p. 11, 2011.

[24] A. Agarwal and A. Agarwal, "The Security Risks Associated with Cloud Computing," International Journal of Computer Applications in Engineering Sciences, vol. 1, no. Special Issue on CNS, p. 3, 2011.

[25] P. R. Kumar, P. H. Raj, and P. Jelciana, "Exploring Data Security Issues and Solutions in Cloud Computing," 6th International Conference on Smart Computing and Communications, ICSCC 2017, vol. Procedia Computer Science, no. 125, pp. 691–697, 2018.

[26] R. Patil, H. Dudeja, and C. Modi, "Designing an efficient security framework for detecting intrusions in virtual

network of cloud computing," Computers & Security, vol. 85, pp. 402–422, 2019.

[27] K. Popović and Ž. Hocenski, "Cloud computing security issues and challenges," in The 33rd International Convention MIPRO, 2010, pp. 344–349.

[28] A. S. Al-Saleh and S. A. Al-Shaya, "Enhancing Cloud Computing Environment: Improving Cloud Computing Applications Performance Using Cloudlet-Based Architecture," International Journal of Wireless Communications, Networking and Mobile Computing, vol. 4, no. 5, pp. 38–43, 2017.

[29] R. Velumadhava R., "Data security challenges and its solutions," presented at the International Conference on Intelligent Computing, Communication & Convergence, 2015, pp. 204–209.

[30] M. Zhao and Y. Geng, "Homomorphic encryption technology for cloud computing," in 8th International congress of information and communication technology, ICICT 2019, 2019, vol. 154, pp. 73–83.

[31] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, vol. 28, no. 3, pp. 583–592, Mar. 2012.

[32] M. Okuhara, T. Shiozaki, and T. Suzuki, "Security Architectures for Cloud Computing," FUJITSU Science & Technology Journal, vol. 46, no. 4, pp. 397–402, 2010.

[33] S. Gupta, P. Kumar, and A. Abraham, "A Profile Based Network Intrusion Detection and Prevention System for Securing Cloud Environment," International Journal of Distributed Sensor Networks, vol. 9, no. 3, p. 364575, Mar. 2013.