A Review on Data Security and Emerging Threats in Cloud Computing

Masese Chuma Benard[1], Muhaise Hussein[2], Turiabe Victor[3], Joel Sadiki Charo[4]

[1] Computing department, Kampala international university- western campus
[2] Faculty of Science and Technology, Kampala international university- western campus
[3] Computing department, Kampala international university- western campus
[4]Kenya Methodist university- Mombasa campus

Abstract: **The advent of cloud computing has become a game changer and paradigm shift for digital services delivery. The cloud service providers enable the end user to access, adopt and use resources, programs and applications where some are free and other are pay as you use. This has reduced the pressure of computing resources and hence increased the processing speed. The infrastructure and storage of alarge amount of data, including important information are some of the striking cons of cloud computing services. The service provider can enable the end users to access software as a service (SAAS), platform as a service (PAAS), and infrastructure as a service (IAAS) and recovery as a service (RAAS). Though cloud computing is viewed a game changer in computing world there are a number of threats and challenges posed by this technology. Therefore, the aim of this paper is to review systematically literature on data security and emerging threats in cloud computing posed from set policies, technology, controls and procedures and categorize the numerous security issues which need to be addressed for example multi-tenancy, shared technology, data availability and integrity**

Keywords: **Cloud Computing, data security, information threats, Challenges of cloud computing. SAAS, PAAS, IAAS**

I. INTRODUCTION

Cloud computing gives users the ability to increase their capabilities dynamically without the need for buying new infrastructure, recruiting new employees, or licensing new software. Shared resources, software, infrastructure, and information are provided to computers and other devices as a utility (like the electricity grid) over a network (typically the internet) (Radwan, Azer, & Abdelbaki, 2017).

With invent of new technologies, we generate a large amount of information on regular basis in the era of big data, security breaching and data mining are the major issues of concerns. (Gupta, Gupta, & Kumar, 2019). Cloud computing is becoming more and more popular nowadays and is increasing in popularity among large companies as they share valuable resources in a cost-effective manner (Radwan, Azer, & Abdelbaki, 2017).

II. METHODS AND MATERIALS

The research used systematic review of academic literature, generalizations and systemization accordingly in respect to the themes relevant to secondary literature, working policy papers, journals and various periodicals were included in the study.

III. RESULTS AND DISCUSSIONS

Cloud computing security threats

Data security and cloud security are gaining attention and many big companies are making regulations and policies in order to deal with security issues. The growing and continuous security breaches have forced government to drive new rules and regulations to take these cyber security and privacy concerns very seriously. Small scale and large-scale industries and public and private sectors are enforced to follow Government norms and standards in order to ensure maintain integrity, availability of digital assets and confidentiality. Heavy penalties are imposed for non-compliance of these security breaches. Encryption and encoding are mandatory for better privacy at enterprise level (Gupta, Gupta, & Kumar, 2019).

Security issues in cloud is a major obstacle for its adoption Security issues can be grouped into sensitive data access, data segregation, privacy, bug exploitation, recovery, accountability, malicious insiders, management console security, account control, and multi-tenancy issues. There are many other challenges and risks in cloud computing that leads to loss of security which has to be taken care in order to build trust in customers about cloud computing technology (Rachana & Guruprasad, 2014).

Security and privacy: As cryptographic approaches and policy rules are the pivotal terms in cloud computing security, both need significant attention. Because existing cryptographic algorithms for cloud security, privacy protection and outsourced computation demands new research directions (Kaur & Singh, 2020).

Security and privacy are considered as a critical issue in a cloud computing environment due to the sensitive and important information stored in the cloud for customers. Critics argue that cloud computing is not secure enough because data leaves companies' local area networks(Hussein & Khalid, 2016).

Shared technology vulnerabilities

IaaS vendors depend on the usage of multi-tenancy property by introducing their infrastructure for sharing. Components such as disk partitions and shared database services, Central

Processing Unit (CPU) cashes, Graphics Processing Units(GPUs) and other elements were designed to be used by a single customer not to pose robust separation properties from multi-tenant architecture (Radwan, Azer, & Abdelbaki, 2017).

According to (Rupra, 2020) in his study noted that cloud computing is not a standalone computing platform because it combines several technologies including networks, operating systems (OS), databases, virtual servers and components, resource scheduling, transaction processing, concurrency control techniques, load balancing, memory management and numerous others for its functionality and operation, a threat in any one of the technologies becomes a threat for the entire cloud platform. This causes a serious security challenge in the implementation of SaaS delivery model.

Privileged access: Data processed outside the enterprises are subject to many risks, because of issues related to data ownership. Enterprises should ask their providers to supply more information about who has privileged access to data and who controls the hiring and management of administrators (Radwan, Azer, & Abdelbaki, 2017).

Data segregation: Most cloud providers store data in a shared environment. Consequently, a provider must deploy a mechanism to separate clients' data. Encryption is not everything, some implementation mistakes may result in exploits or data breaches. Clients must know who has access to the decryption keys and what part of data can be decrypted by every key (Radwan, Azer, & Abdelbaki, 2017).

According (Gill, Razzaq, Ahmad, Almansour, & Haq, 2022) to noted six major security issues are listed below

- Data integrity
- Data privacy and confidentiality
- Location of data
- Availability of data
- Data storage, backup, and recovery
- Data authentication (Khan, et al., 2021).

Security issues in SaaS

In SaaS, the client has to depend on the vendor for proper security paradigms. The provider must do the work to keep multiple users‟ from seeing each other's data. So, it becomes difficult to the user to ensure that right security measures are in place and also difficult to get assurance that the application will be available when needed SaaS provides application services on demand such as email, conferencing software, and business applications such as ERP, CRM, and SCM. SaaS users have less control over security among the three fundamental delivery models in the cloud. The adoption of SaaS applications may raise some security concerns (Hammouri & Mirza, 2016).

Security issues in SAAS

SAAS challenges	Characteristics	End products	Examples	authors
Authentication and authorization Data confidentiality Availability Information security Data access Data breaches Identity management and sign on process	Web access to commercial software. Software managed from a central location. Software delivered in a "one to many" model. Users not required to handle software upgrades and patches. Application Programming Interfaces (APIs) makes integration between different pieces of software possible.	Software Application	Salesforce.Com, CRM, Sugar CRM, GMail, Microsoft Office365, Lync Online, Exchange Online, Share point Online	(Hussein & Khalid, 2016; Kumar & Vajpayee, 2016)

Security issues in PAAS

PAAS	characteristics	Examples	End products	Authors
Data location Privileged access Distributed systems	Multi-tenant architecture. Customizable /Programmable User Interface. Unlimited Database Customization. Robust Workflow engine/capabilities. Granular control over security/sharing (permissions model) Flexible "services-enabled" integration model.	SaaS Grid, Google-App engine, Froce.Com, Bungee, Heroku, Web Role, Work Role, Map Reduce, Blob, Message Queue, Service Bus, Cloud front, Marketplace	Framework for Developing Applications,	(Hammouri & Mirza, 2016; Mehmood, Roman, Umar, & Song, 2015)

IaaS offers computation, storage and communication as virtualized resources. Instead of purchasing servers, software and network resources these resources are rented by the customers of cloud computing on demand and billed for these resources as per usage. By paying to the IaaS providers customers are allowed to create virtual servers on their infrastructure. Unlike other two services customers of IaaS are responsible for setting and managing applications, run time,

data, OS and middleware. IaaS provides virtualization, servers, hard drives, storage and networking as a service (Mehmood, Roman, Umar, & Song, 2015).

The users of IaaS are usually it department who save their cost by renting a fully outsourced infrastructure for which they do not need to worry about updating, upgrades and maintenance. The customers are changed based on CPU hours, gigabytes of storage and network bandwidth used by the customers if IaaS(Mehmood, Roman, Umar, & Song, 2015).

IAAS	CHARATERISTICS			
	Service Level Agreement (SLA) • Dynamic scaling • Automation of administrative tasks • Utility computing service and billing model • Internet connective • Desktop virtualization	EC2, GoGrid, Mosso, FlexiScale	Computer Infrastructure, Storage, Networking	(Mehmood, Roman, Umar, & Song, 2015)

Data Security Issues And Emering Threats In Cloud Computing

Challenges	**Model**	**Description**	**Significance**	Authors
Data availability	service provider agreement framework	SLA parameters and flexible negotiation methods	Manage the appropriate emergency response and plan and unplanned	(Khan, et al., 2021)
Data Storage	Data storage framework PaaS	combine and extend multiple databases and.	user centric trust model to help users to manage the storage	(Kaur & Singh, 2020)
Integrity	MAC algorithms.	The owner of data must Import the outsourced data and then measure	Unplanned and expected changes will be noted	(Khan, et al., 2021)
Security	Hidden Markov Model (HMM)	detect any type of security breach	identify security in cloud computing network.	(Gill, Razzaq, Ahmad, Almansour, & Haq, 2022)
dos				(Hussein & Khalid, 2016)
EMERING THREATS IN CLOUD COMPUTING				
THREATS	Service model affected	DESCRIPTION	Challenges	AUTHERS
Data leakage	SAAS, PAAS	Data leakage happens when the data gets into the wrong hands while it is being transferred, stored, audited or processed	Trust issue with the cloud providers. · Untested procedures, standards, and insufficient data preservation methods. · Absence of knowledge.	(Kumar & Vajpayee, 2016; Alhenaki, Alwatban, Alahmri, & Alarifi, 2019)
Denial of Service	SAAS, PAAS, AND IAAS	DoS attacks are the most prominent attacks in the CC environment. The main aim of the attacker is to exhaust all the resources of the victim by sending thousands of request packets to the victim over the Internet DoS attacks target the availability of the services provided by the cloud in order to flood a network. Thus, they reduce the user's bandwidth, disrupt service to a specific system, and prevent the user from accessing or using the cloud service.	Service availability is affected; a fake service may be created	(Alhenaki, Alwatban, Alahmri, & Alarifi, 2019)
Account or service hijacking	SaaS, PaaS	An account theft can be performed by different ways such as social engineering and weak credentials. If an attacker gains access to a user's credential, he can perform malicious activities such as access sensitive data, manipulate data, and redirect any transaction	· Fast growth of CC opens new gaps. · Current method of digital identity management is not good enough for hybrid clouds.	(Kumar & Vajpayee, 2016; Alhenaki, Alwatban, Alahmri, & Alarifi, 2019)
Data manipulation	SAAS, PAAS			
Sniffing/Spoofing virtual networks	SAAS, PAAS	A malicious VM can listen to the virtual network or even use ARP spoofing to redirect packets from/to other VMs		(Kumar & Vajpayee, 2016)

Shared-Technology Vulnerabilities	IaaS		· Development of shared components is not guaranteed. · The use of VM technology. · Mapping between the manufacturing process and allotment process of shared components.	(Radwan, Azer, & Abdelbaki, 2017)
Malicious Insiders		The malicious-insider threat arises from trusted people within the cloud organization who have authorized access to the organization's assets and items of value.	· Providers hide their company strategies from employees. · Lateness of solutions, developed after the incident occurs. · Incapability of cloud providers to monitor employees	(Alhenaki, Alwatban, Alahmri, & Alarifi, SECURITY IN CLOUD COMPUTING: A SURVEY, 2019)

Three forms of cryptography algorithms (i) Hashing. (ii) Symmetric algorithms (iii) Asymmetric algorithms

Symmetric Key Cryptography

"Secret Key Encryption Algorithm" (Symmetric algorithm), the only private key is used for encoding and decoding. These algorithms are separated for 2 types: Block and Stream cipher Input are taken as a block of fixed sizeplaintext is taken of fixed size in block cipher consequently to the type of asymmetric encryption algorithm, thefixed-size key is implemented on plain text block and then same size the output block as plaintext is acquired. At atime one bit is encoded in case of Stream Cipher. The usefulness of utilizing Symmetric-key encryption is that it actually works with high speed in encryption anddoes not excessively use computation powerAES, DES, BLOWFISH, RC5, and 3DES some of the regular symmetric key algorithms(Zaineldeen & Ate, 2020).

Data Encryption Standard

Features:

Block size = 64 bits

– Key size = 56 bits (in reality, 64 bits, but 8 are used as

parity-check bits for error control, see next slide)

– Number of rounds = 16

– 16 intermediary keys, each 48 bits

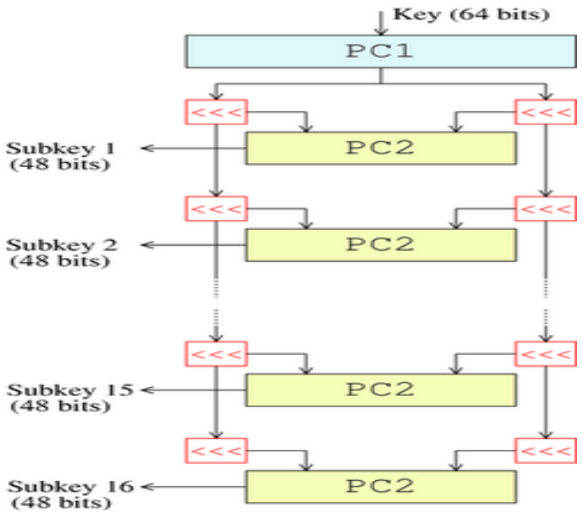

Fig: The key-schedule of DES

Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) it was selected from a candidate list in a multiple round selection. The first round chose algorithms with the best performance on personal computer systems while the second round chose algorithms with the best performance on field programmable gate arrays. Therefore, the AES cryptosystem has great performance and acceleration abilities. The AES encryption includes these functions, Sub Bytes, Shift Rows, Add Round Key, and Mix Columns for the data manipulation. AES system goes through10 rounds for 128-bit keys, 12 rounds for I92-bit keys, and 14rounds for 256-bit keys depend on key size, to transfer final cipher text or to get back the original text (Saeed, Zakiah Ayop, & Baharon, 2018).

Asymmetric Key Cryptography

Asymmetric – double unique keys are utilized. The public key is accessible to anybody on the network. The public key gets utilized to encode data. The only private key can decode that data. The private key is reserved secret and intended in keeping information secure(Zaineldeen & Ate, 2020).

The pros of utilizing asymmetric key encryption are that it gives better scalability and distribution of key relative to symmetric systems. A few standard Asymmetric Key Algorithms are El Gamal, ECC, RSA, DSA, Diffie-Hellman. The asymmetric encoding algorithm needs more computational processing power if we evaluate it compare to symmetric encoding algorithm. Symmetric approximately 1000 times faster compare to Asymmetric techniques (Zaineldeen & Ate, 2020).

Paper/literature sources

Digital libraries	Identified papers published	Pre-selection	selected
IEEE	78	23	9
Google scholar	14,121	137	27
Springer link	1201	56	12
ACM	2100	28	6
Total	17,500	244	54

Paper Selection Criteria

The research reviewed 244articles systematically. Then 54 articles were selected based on the theme and relevance to the study. Though some of the excluded article contained some concept to the study but they were not included in the study. Those paper that did not match the keywords with ourresearch string. Duplicate papers will also be excluded. Those papers that are not written in English language.

IV. CONCLUSION

Conclusion

Cloud computing has developed and adopted fast and hence has changed the computing paradigm both in academic and corporate digital world. It introduces big data storage and capacity with flexible scalable computing processing power to match different demands and supply through the internet. Cloud users can have the benefit of reduced costs in computing devices. The security of the data is provided by the service providers. It has been noted that that Privacy, Confidentiality, Availability of services data, Integrity of data is the major concern while adopting and using cloud computing this is a result of the security model adopted by service as a service which give room for hacker to penetrate, also the multi-tenancy in the cloud a major issue for clients due to the possibility of a hacker taking advantage of the same host.

REFERENCES

[1] Alhenaki, L., Alwatban, A., Alahmri, B., & Alarifi, N. (2019). SECURITY IN CLOUD COMPUTING: A SURVEY. International Journal of Computer Science and Information Security (IJCSIS), 67-90.

[2] Gill, S. H., Razzaq, M. A., Ahmad, M., Almansour, F. M., & Haq, I. U. (2022). Security and Privacy Aspects of Cloud Computing: A Smart Campus Case Study. Intelligent Automation & Soft Computing, 117-128.

[3] Gupta, D., Gupta, K., & Kumar, N. (2019). EMERGING TECHNOLOGIES AND TRENDS IN CLOUD. COMPUSOFT, An international journal of advanced computer technology, 3146-3149.

[4] Hammouri, A., & Mirza, I. (2016). Analysis of Critical Security Challenges in Software as a Service of cloud computing. International Journal of Computer Science and Information Security (IJCSIS), 547- 555.

[5] Hussein, N. H., & Khalid, A. (2016). A survey of Cloud Computing Security challenges and solutions. International Journal of Computer Science and Information Security (IJCSIS),, 52-56.

[6] Kaur, A., & Singh, G. (2020). Cloud Computing Security Issues and Challenges. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 265-270.

[7] Kumar, S. N., & Vajpayee, A. (2016). A Survey on Secure Cloud: Security and Privacy in Cloud Computing. American Journal of Systems and Software, 14-26.

[8] Mehmood, A., Roman, M., Umar, M. M., & Song, H. (2015). Cloud Computing Security: A Survey. (IJCSIS) International Journal of Computer Science and Information Security, 20-28.

[9] Rachana, S. C., & Guruprasad, H. S. (2014). Emerging Security Issues and Challenges in Cloud Computing. International Journal of Engineering Science and Innovative Technology (IJESIT), 485-490.

[10] Radwan, T., Azer, M. A., & Abdelbaki, N. (2017). Cloud computing security: challenges and future trends. International Journal Computer Applications in Technology, 158–172.

[11] Rupra, S. S. (2020). A Descriptive Research on the Security Challenges of Cloud Computing Among Selected SMEs in Kenya. International Journal of Innovative Science and Research Technology, 588-598.

[12] Saeed, Z. R., Zakiah Ayop, N. A., & Baharon, M. R. (2018). Improved Cloud Storage Security of Using Three Layers Cryptography Algorithms. International Journal of Computer Science and Information Security (IJCSIS),, 34-39.

[13] Zaineldeen, S., & Ate, A. (2020). Review of Cryptography in Cloud Computing. International Journal of Computer Science and Mobile Computing, 211-220.