

NAME: ADELEKE DAVID TEMITOPE

COURSE: CLOUD AND NETWORK SECURITY

MOODLE: RESEARCH METHOD

ASSIGNMENT: RESEARCH PROPOSAL

STUDENT ID: 2316994

MOODLE NO: SWE7004

LECTURER: Dr. Celestine Iwendi

DATE: March 15, 2024

(DATA SECURITY AND PRIVACY PROTECTION IN MULTI-TENANCY CLOUD COMPUTING ENVIRONMENT)

Table of Content

Contents

[1.0 Problem Statement 3](#_Toc161179974)

[1.1 Introduction 3](#_Toc161179975)

[1.2 Aim 3](#_Toc161179976)

[1.3 Background 3](#_Toc161179977)

[2.1 Research Questions 4](#_Toc161179978)

[2.2. Research Objectives 4](#_Toc161179979)

[2.3. Research Design 4](#_Toc161179980)

[3.0. Methodology 5](#_Toc161179981)

[3.1. Data collection and interpretation 5](#_Toc161179982)

[3.2. Quantitative Data/Analysis 5](#_Toc161179983)

[3.3. Qualitative Data/Analysis 5](#_Toc161179984)

[3.4. Quantitative/ Qualitative Data Analysis 6](#_Toc161179985)

[4.0. Reflection 6](#_Toc161179986)

[4.1. Implication and Contribution to knowledge 6](#_Toc161179987)

[4.2. Conclusion 6](#_Toc161179988)

[5.0 References 7](#_Toc161179989)

Table of Figure

[Figure 1: Zero Trust Security 5](#_Toc161179290)

# 1.0 Problem Statement

Cloud computing has offered a more effective and efficient way of carrying out daily business activities with the ease of scalability and faster processing of users’ data to give quicker result. The hindrance to the wide acceptance of cloud computing is the non-scalable security and privacy protection of the users’ data in a multi-tenancy environment where it is difficult for Cloud Service Provider (CSP) to identify vulnerable tenants within the cloud environment, security threat-prone application installation by users and non-dynamic protection mechanism (Sun, 2019).

# 1.1 Introduction

The advent of cloud computing with the intent of providing scalability, reliability, flexibility and on-demand services to customers has caused to businesses and organizational operations to thrive without the business owners concerned with the hassles of how to set up data centers for operations, cost implications, scalability and security concerns (Bello et al., 2021). The accommodation of many users in the cloud environment to share the same resources has subjected the public cloud environment to a lot of security threats and privacy invasion that translates in data loss, integrity issues, confidentiality breaches and availability denial, which is serving as hindrance to full adoption and acceptance of cloud computing system (Waghmare et al., 2021).

Keywords: Security threat, confidentiality, data loss integrity issue

# 1.2 Aim

The data traffic from multiple tenants and from different sources into the cloud computing environment makes the environment security threat-prone and privacy protection breach of other innocent tenants inevitable (Sun, 2020). This research seeks to suggest a different approach to data security and user privacy protection in a cloud environment of many tenants.

# 1.3 Background

The increasing users of cloud environment resources because of its immerse benefits of agility, scalability and cost effective has also caused the increase in data security and privacy breaches for both the provider and the users of the multi-tenancy cloud services (Hongling, 2019).

# 2.1 Research Questions

1. How can robust threat identification and isolation mechanism be implemented within a multi-tenant cloud computing environment?
2. What are the implications of security and privacy breaches associated with multi-tenancy cloud computing?
3. What dynamic mechanism can be adopted to verify users’ installation intended application to ascertain threat or vulnerability free?
4. How can zero-trust security be implemented at every level of data access, retrieval and storage by users to enhance the security and privacy within multi-tenancy cloud computing?
5. To what extent is the effectiveness and efficiency of the existing user authentication and access control in providing data security and privacy in a co-tenant cloud environment?

# 2.2. Research Objectives

1. To examine the existing security and privacy protection mechanisms employed and implemented in cloud computing environments.
2. To propose robust mechanisms that will mitigate vulnerable tenant-influenced security and privacy breaches in a multi-tenancy cloud computing environment.
3. To implement zero-trust security and privacy protection mechanism to verify and validate users at every level of operations within the cloud computing environment.
4. To examine the policies and legal regulations guiding the collection, processing and storage of tenants’ data in multi-tenancy cloud computing.

# 2.3. Research Design

Figure 1 shows the levels data security and protection from one point to the other to achieve a zero-level trust on every user in a multi-tenancy cloud environment. The tenants are first verified before being granted access and the second level is the encryption of data to and from the cloud storage to provide privacy of the data.

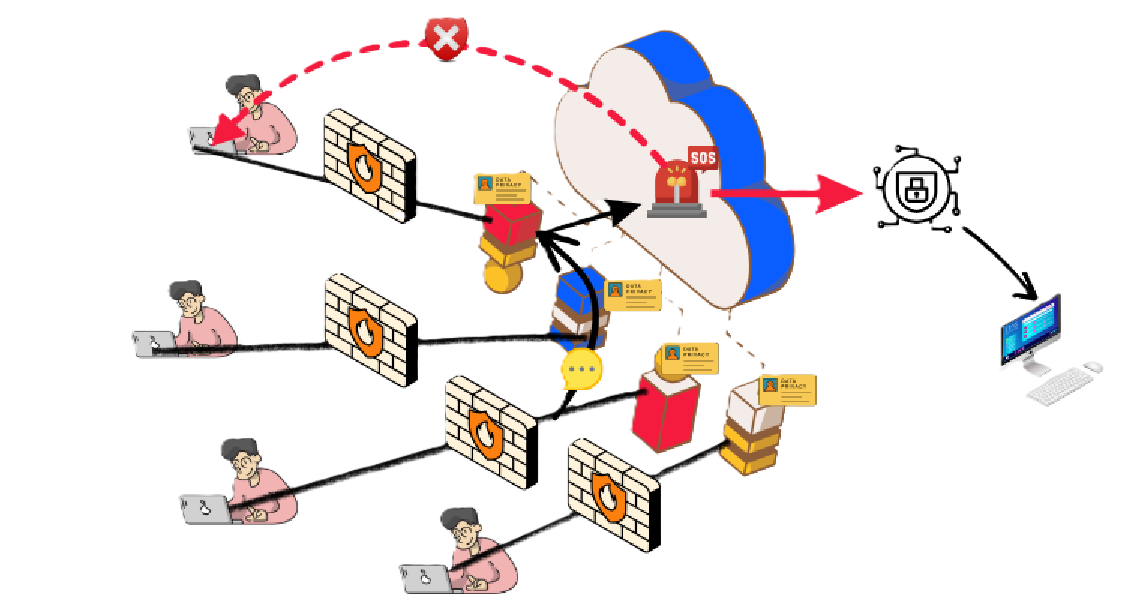


Figure 1: Zero Trust Security

# 3.0. Methodology

## 3.1. Data collection and interpretation

The process of data collection and interpretation is a deliberate action which requires proper planning on who is the target audience for the data collection, developing a prototype question sample to simulate for the real experience. The real-life questionnaires that would be needed for the research purpose, training on its administration and equipment needed for the administration. The field work deals with meeting the target audience for the data collection and assuring them of their privacy protection. The last phase is the data analysis using any preferred tool and making the final report (World Health Organization and United Nations Children’s Fund (UNICEF), 2019).

## 3.2. Quantitative Data/Analysis

To generate a generalized report on the issues bothering on data security and privacy based on figures made available as secondary data source. This data would help to examine different forms of threats and privacy breaches, the limitations and strengths of their methodologies (Coy, 2019).

## 3.3. Qualitative Data/Analysis

To conduct a survey on the users of cloud platform services for business or personal usage to gather what has been their sense of security and privacy protection experiences, how was the privacy protection breached and the causative effects (Coy, 2019). To implement the Zero Trust approach, the feelings and experiences of users on being requested for authentication at every level of application usage must be known.

## 3.4. Quantitative/ Qualitative Data Analysis

The combination of these two would help to broaden the scope of results, enlarged look on the research methodology and the effects on users, and it will enhance more accurate decision making.

# 4.0. Reflection

My reflections on this assessment are as follows; through this assessment, I have learnt how to review a paper within 5 – 10 minutes and grasp its purpose, concepts, and methodology. This assessment has helped to inform me how to develop new concepts from other peoples’ concepts. It has improved my design skills for a proposed solution, and it has helped me in the formulation of right objectives regarding a research topic or area.

## 4.1. Implication and Contribution to knowledge

* Behavioral – the research would help to extract user feeling and experience, and for user to know his or her roles in data security and privacy protection while using a multi-tenancy cloud computing platform.
* Organizational - the research would inform Cloud Service Providers (CSPs) on what are the limitations to their existing security measures, what new approach to take on their customers’ data security and their privacy protection.
* Academic – the research would open opportunities to other academic writers to explore any shortfalls in the aspect of implementation and methodology to deliver additional work that would improve data security and privacy protection of users in multi-tenancy cloud computing environments.

## 4.2. Conclusion

This research would examine identify the different form of data security threats, understudy various ways that users of multiple tenants’ cloud platforms have experienced privacy breaches, the effects of the action on them as individuals or their businesses. Also propose a methodology of Zero Trust as another way of data security and privacy protection for users of public cloud computing platforms.

# 5.0 References

Bello, S.A., Oyedele, L.O., Akinade, O.O., Bilal, M., Davila Delgado, J.M., Akanbi, L.A., Ajayi, A.O., Owolabi, H.A., 2021. Cloud computing in construction industry: Use cases, benefits and challenges. Automation in Construction 122, 103441. https://doi.org/10.1016/j.autcon.2020.103441

Coy, M., 2019. Research Methodologies: Increasing Understanding of the World. International Journal of Scientific and Research Publications (IJSRP) 9, p8511. https://doi.org/10.29322/IJSRP.9.01.2019.p8511

Hongling, L., 2019. Research on Solutions to Privacy Security Problems Based on Big Data, in: 2019 11th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA). Presented at the 2019 11th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), IEEE, Qiqihar, China, pp. 585–588. https://doi.org/10.1109/ICMTMA.2019.00134

Sun, P., 2020. Security and privacy protection in cloud computing: Discussions and challenges. Journal of Network and Computer Applications 160, 102642. https://doi.org/10.1016/j.jnca.2020.102642

Sun, P.J., 2019. Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and Solutions. IEEE Access 7, 147420–147452. https://doi.org/10.1109/ACCESS.2019.2946185

Waghmare, V., Khandve, H., Kamble, N., 2021. Privacy in Multi-Tenancy Cloud. International Journal of Innovative Research in Computer and Communication Engineering 9, 14498. https://doi.org/10.15680/IJIRCCE.2021.0911022

World Health Organization, United Nations Children’s Fund (UNICEF), 2019. Recommendations for data collection, analysis and reporting on anthropometric indicators in children under 5 years old. World Health Organization, Geneva.