International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 11 Issue 8 ǁ August 2023 ǁ PP. 33-38

Security in the Cloud: Challenges and Solution

Zaldy B. Eledia Jr., Ryan Jay Guinto, Kristine T. Soberano
Northern Negros State College of Science and Technology, Philippines
Corresponding email: zaldyelediajr.1835@gmail.com

ABSTRACT
In recent years, cloud computing has gained popularity and is now used to support various areas of human life. Security in the cloud is a crucial aspect to consider when utilizing cloud computing services. Cloud security refers to the policies, procedures, and technologies implemented to protect cloud-based systems, data, and infrastructure from unauthorized access, data breaches, and other cyber threats. Cloud computing has become increasingly popular in recent years due to its scalability, flexibility, and cost-effectiveness. However, as organizations continue to store more sensitive data in the cloud, the needs for effective cybersecurity measures become increasingly critical. In this paper, we will explore the challenges faced by organizations in securing their cloud environments and discuss potential solutions to these challenges. From identifying potential threats to implementing secure data access controls, this paper aims to provide a comprehensive overview of the challenges and solutions for cybersecurity in the cloud.

Date of Submission: 01-08-2023 Date of acceptance: 12-08-2023

I. INTRODUCTION

The internet's expansion is undoubtedly widespread and has developed an innovative environment. With the help of the internet, online transaction has been developed, allowing the information process much faster. Cloud Computing provides a way to store and access cloud data from anywhere by connecting the cloud application using the internet by choosing the cloud services the users are able to store their local data in the remote data server [1]. Therefore, users' anxiety about the safety of Cloud computing is reasonable. For example, the operation management of a user's system can be entrusted to a provider in a public Cloud. However, a user may not understand a provider's detailed operation management method. Generally, in the Cloud environment, the operation is managed by using virtual technology as the base in many cases in the multi-tenant form in which two or more users share the system environment[2]. Cloud computing technology covers a large area of services in sharing systems in different and distributed situations with software and hardware points, Collection and sharing of data in large systems caused problems in security to save the system from damage and attack[3].

Security in the cloud was a big help for us when it comes to security, access files, and efficiency especially for the IT industry, for all beneficiaries, and also to make storing important files. The cloud gives you access to more applications, improves data accessibility, helps your team collaborate more effectively, and provides easier content management. Some people may have reservations about switching to the cloud due to security concerns, but a reliable cloud service provider (CSP) can put your mind at ease and keep your data safe with highly secure cloud services. In this case the security in the cloud: challenges and solution. Cloud computing provides an efficient way for operators to maintain data, services, and applications by bringing technologically distinct systems into a single domain on which multiple services can be deployed to achieve higher flexibility and availability with less CapEx and OpEx [4].

Data in a cloud requires its own protection, particularly data separation in the cloud service to secure data. Data separation can be accomplished at different levels by virtualization, encryption, and authentication. That enhances data security from an unauthorized person [5].

The researchers show the evolution of cloud computing and how cloud computing demand services, and stability very economically.

Mainframe Computing	**SMP/open Systems**	**Distributed Computing**	**Grid Computing**	**Cloud Computing**
Aforementioned Core memory, mass-storage devices, computer graphics systems (for plotting the aircraft)	pool of homogeneous processors, independent administered software	web-based application, multitier architecture	Providing virtualization of distributed resources	computin IaaS PaaS SaaS

60s, 70s **80s,90s** **Late 90s** **Early 2000** **Late 2000**

Figure 1 The computing architecture evolution

Conceptual Framework

The researchers conducted a study on how security in the cloud is demand services, the innovation of backup strategies, and how it is effective and user needs**.**

The input-process-output (IPO) model. The Input phase is to store User information or Data in the Cloud Security Storage. In the Process phase, the system gives the user information that your data is secured and stored. The output phase is the system functionality.

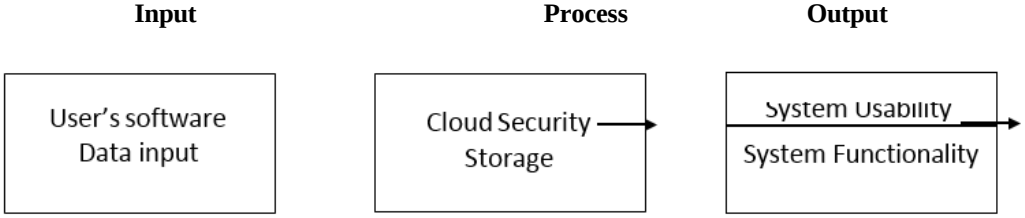


Figure 2 The Conceptual Framework of the Study

II. Methodology

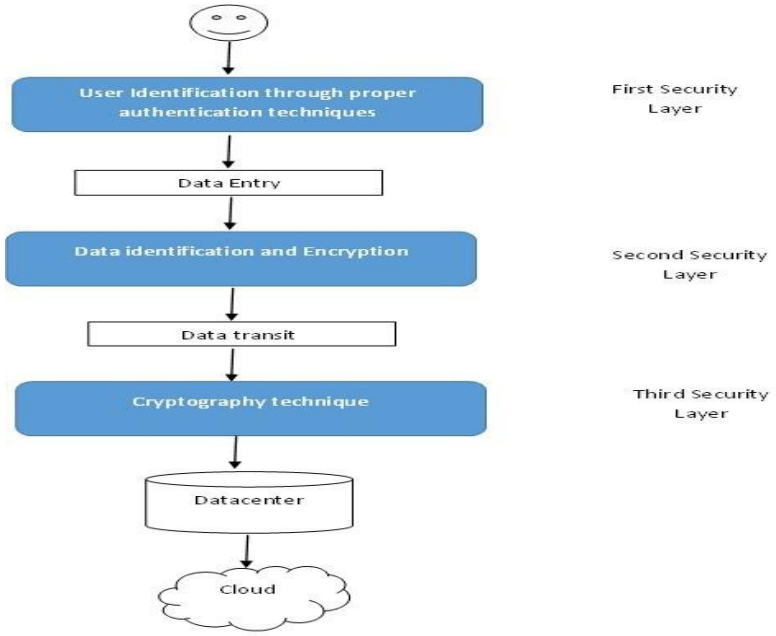
2.1 Research and Design

The research design refers to the overall strategy and analytical approach that you have chosen in order to integrate, in a coherent and logical way, the different components of the study, thus ensuring that the research problem will be thoroughly investigated. It constitutes the blueprint for collecting, measuring, and interpreting information and data [6].

This study thoroughly discusses methods and strategies appropriate for conducting design and development research [7].

2.2 V- Proposed Model

The proposed cloud security model is composed of three layers. In the first layer user's identification can be checked through proper authentication techniques. Security in the second layer depends on data identification and encryption. At the last layer cryptography technique is used to secure the transmission of the data [8].



2.3 Software Development Life Cycle

To have maximum productivity in the development of new technology, it is needed to adapt them with related models and methods. So, to increase the productivity of software development in the cloud, there should be a matching between the cloud and the software development lifecycle (SDLC). There are several software development lifecycle models in software engineering [9].

There are many activities and practices are proposed to achieve the security goals of the enterprise. In this paper, we proposed an integrated security testing framework for a secure software development life cycle [10]. Specifically, this study used the Rapid Application Development or RAD Model.

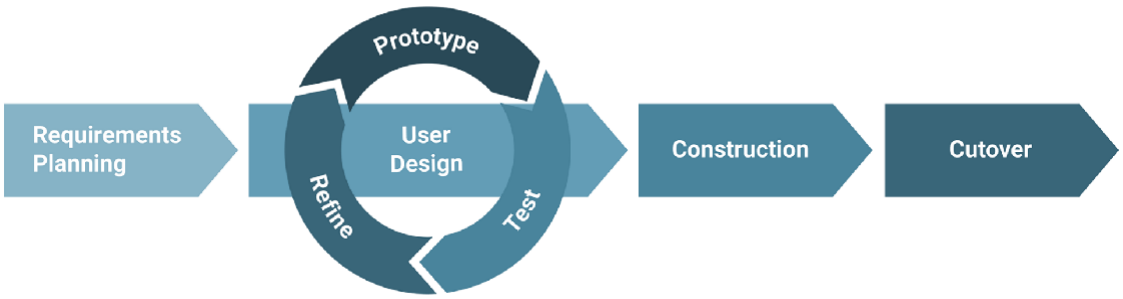


Figure 3 Rapid Application Development Model

Figure 2.0 Input, Process, and Outcome show the Prototype of the Model used by the researchers for the development of the system. This kind of prototype model needs to be shown or followed to meet the requirements to have a better outcome for developing a system.

Requirements Planning

In this stage of requirements planning, the researchers define and document the project's requirements. This involves identifying the stakeholders and their needs, gathering information about the project goals and objectives, and analyzing the information to create detailed requirements documents. It is important to involve stakeholders, such as users, developers, and project managers to ensure that everyone has a clear understanding of the project goals and objectives and that the requirements are feasible and realistic.

Data Analysis

The researchers need to conduct studies to define the problem or question that needs to be answered. In this step, researchers help ideas or concepts to give a direction on how the system builds and implemented then give the satisfaction that the users need.

System Design

The researchers start to make and then develop a proposed system. It requires careful planning, analysis, and design to ensure that the resulting system meets the needs and performance. An essential process in software engineering and is critical to the success of any software project. It involves a careful balance of trade-offs between various factors, such as performance, scalability, and cost, to deliver a system that meets the needs of its users while remaining feasible to implement and maintain.

Prototype Cycle

In this stage, the researcher starts the process of designing, building, and testing prototypes of a product or service. This process involves several stages, which may vary depending on the specific design methodology used.

Testing

Once the design is completed, it is important to create prototypes and test the system to ensure that it meets the requirements of its stakeholders. This can involve creating a test case to rate the stakeholders as well as performing functional and performance testing.

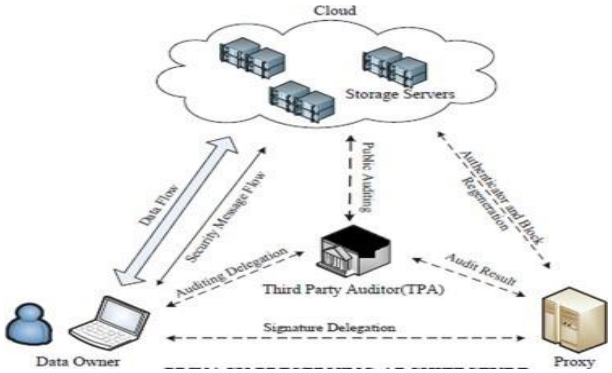
Implementation and Deployment

In software development, coding and testing of a software program, which involves turning a design or concept into a functional software application. In project management, implementation involves putting a project plan into action and executing the tasks necessary to complete the project successfully.

2.3 Framework

Data flow diagram (DFD) was the tool used to develop the framework. DFD is a graphical modeling tool that breaks down complex systems into a network of functional processes[11]. Generally, a Data Flow Diagram use symbols to provide a graphical representation of the information flows through a process.

Figure 4 The Context Data Flow Diagram of the Develop System



III. PRESENTATION OF DATA SECURITY CHALLENGES, AND SOLUTION

3.1 Cloud security challenges and Potential Solutions for cloud technology

Table 1 shows the result of the researcher conducting a survey on how the security cloud made this possible solution to that particular problem. The studies analyze the risks and threats and often give recommendations on how they can be avoided or covered, resulting in a direct relationship between vulnerability or threats and possible solutions and mechanisms to solve them [12]. Most of the approaches discussed Security Issues, Attacks/Issues, Impact on cloud systems, and Countermeasures/possible solutions. A number of vulnerabilities and threats are focused on Cloud computing. In addition, we can see that in our search, many of the approaches, in addition to speaking about threats and vulnerabilities, also discuss other related issues to security in the cloud such as data security, trust, or security recommendation and mechanism for any problems encountered in these environments.

Table 1: Common technical security issues in cloud computing and their highly efficient possible solution.

Security Issues	Attack / Issue Definition	Impact on Cloud System	Countermeasures/ Possible solutions
XML Signature Wrapping attacks	Insert new Body to the original message	Original data information changed	Use secure coding
Browser Security	Data is stored passively so the browser can't generate authentication tokens	This leads to data loss	Use xml signature
Lock in	Complexity issue in moving from one platform provider to another platform provider	Vendor lock-in clients.	-Middleware -Software adoption -Model-Driven architecture

3.2 Level of Functionality of the developed System in terms of its Security, Accuracy, threats, confidentiality, and Authentication issues.

Table 2 shows the mean and interpretation results from the stakeholder's feedback on the functionality of the developing a system in terms of Security, Accuracy, Threats, Confidentiality, and Authentication Issues compose with the following mean: In Security (M=9.45) interpreted as "Excellent", Accuracy (M=8.95) interpreted as "Excellent", Threats (M=9.27) interpreted as "Excellent", Confidentiality (M=10.00) interpreted as "Excellent", Authentication Issues (M=9.11) interpreted as "Excellent". Overall, the outcome of our system is Excellent and to make sure the needs and wants of users, stakeholders, etc. to meet the satisfaction. Therefore, the innovative features of security in the cloud all the challenges, is to give a better solution. Because every problem has a solution.

Table 2: Level of Functionality of the developed System in terms of its Security, Accuracy, threats, confidentiality, and Authentication issues.

Implementation Indicatiors	Mean	Verbal Interpretation
Security	9.45	Excellent
Accuracy	8.95	Excellent
Threats	9.27	Excellent
Confidentiality	10.00	Excellent
Authentication Issues	8.11	Excellent

Rating Scale: *1.00 -1.99 (Very poor); 2.00 – 3.99 (Poor); 4.00 – 5.99 (Average); 6.00 – 7.99 (Good); 8.00 – 10.00 (Excellent)*

IV. CONCLUSION

The Internet is very important for us, especially for improving the economy, helping people organize, collaborate and share information with large numbers of people, and also creating innovation in our technology which means our lifestyle is made easy but there are some cases, of many human beings on this earth without knowing how the importance of the security of our files because there is some data loss due to human error, hardware failure, or natural disaster which can cause a big problem. The researchers are conducting studies regarding this matter of cloud security to make give importance, especially to society and share with us our innovative ideas to avoid a problem.

The researchers that gathered information including survey, it is important to implement systems because the cloud is a complex and ever-evolving topic that requires continuous attention and adaption. While cloud providers implement various security measures to protect the customer's data, it is ultimately the responsibility of the users to ensure that their data is secure. It's also important to conduct regular security assessments and penetration testing to identify vulnerabilities in the cloud environment and address them promptly. Overall cloud security involves a range of technologies, policies, and procedures that work together to protect cloud resources from authorized access, data breaches, and other security threats.

REFERENCES

[1]. R. V. Rao and K. Selvamani, "Data security challenges and its solutions in cloud computing," Procedia Comput Sci, vol. 48, pp. 204–209, 2015.

[2]. S. Tanimoto, M. Hiramoto, M. Iwashita, H. Sato, and A. Kanai, "Risk management on the security problem in cloud computing," in 2011 First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering, IEEE, 2011, pp. 147–152.

[3]. S. Alatawi, A. Alhasani, S. Alfaidi, M. Albalawi, and S. M. Almutairi, "A survey on cloud security issues and solution," in 2020 International Conference on Computing and Information Technology (ICCIT-1441), IEEE, 2020, pp. 1–5.

[4]. I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G security challenges and solutions,"

IEEE Communications Standards Magazine, vol. 2, no. 1, pp. 36–43, 2018.
[5]. I. Zulifqar, S. Anayat, and I. Kharal, "A Review of Data Security Challenges and their Solutions in Cloud Computing.," International Journal of Information Engineering & Electronic Business, vol. 13, no. 3, 2021.
[6]. R. S. Osalla, D. L. Datolayta, and K. T. Soberano, "Web-based Vaccination Mapping and Profiling with SMS Support: Its Usability to Health Workers in One City in the Philippines," 2023. [Online].Available: www.ijres.org
[7]. R. C. Richey and J. D. Klein, Design and development research: Methods, strategies, and issues. Routledge, 2014.
[8]. N. H. Hussein and A. Khalid, "A survey of cloud computing security challenges and solutions,"International Journal of Computer Science and Information Security, vol. 14, no. 1, p. 52, 2016.
[9]. H. Kashfi, "Software engineering challenges in cloud environment: Software development lifecycle perspective," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 2, no. 3, pp. 251–256, 2017.
[10]. Y.-H. Tung, S.-C. Lo, J.-F. Shih, and H.-F. Lin, "An integrated security testing framework for secure software development life cycle," in 2016 18th Asia-Pacific Network Operations and Management Symposium (APNOMS), IEEE, 2016, pp. 1–4.
[11]. H.-Y. Chong and A. Diamantopoulos, "Integrating advanced technologies to uphold security of payment: Data flow diagram," Autom Constr, vol. 114, p. 103158, 2020.
[12]. K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," Journal of internet services and applications, vol. 4, pp. 1–13, 2013.