APPLICATION OF CLOUD SECURITY IN ENHANCING THE CONFIDENTIALITY, INTEGRITY & AVAILABILITY OF DATA

Bartholomew Idoko[1], Samuel Olofu[1], Kenneth Nwankwo[1], Chinonso Ugwuanyi[1]
[1]Department of Computer Science, Federal Polytechnic Ohodo, Enugu, Nigeria.
bartholomew.idoko@fedpod.edu.ng, samuel.olofu@fedpod.edu.ng,
kenneth.nwankwo@fedpod.edu.ng, eugene.ugwuanyi@fedpod.edu.ng
+234 807 757 7252, +234 7065020184

Abstract:
In this paper, we proposed a system that can enhance the security of data transfer between the cloud and user. Due to security concerns, the majority of enterprises are hesitant to fully trust public or community clouds; some may even consider implementing a hybrid cloud for operations that are more secure. They can store only sensitive data on a relatively small private cloud without jeopardizing the security of critical data. To optimize resource usage, the remaining less sensitive data might be stored on a communal or public cloud. The proposed security solution is a cloud based chat application where information transferred among group of users in real-time are being monitored and protected. The uniqueness of this system is that, it ensures security on both server, client and device ends. The system is designed using the java programming language enterprise edition 21 (Java 21) with the use of Apache Netbeans 21 because the Java application supports web socket with the best security features. The proposed system was implemented, tested and recommended for organizations and individuals that uses cloud based web exchange services.

Keywords: Cloud, security, data, server, Network.

I. INTRODUCTION

Based on the services it provides, cloud computing can be divided into three categories namely; Software as a Service, Platform as a Service and Infrastructure as a Service (Armbrust, et al., 2019).

a. Software as a Service (SAAS): It is the application's delivery service in cloud computing, with SAAS, users are given access to an entire program that is hosted on cloud infrastructure (Buyyaa, et al., 2020). Customers do not need to purchase, install, or maintain hardware because

software is hosted by the provider. Software application instances are shared as services in SAAS. Cloud Drive, Salesforce.com and Google Docs are a few instances of Software as a Service (SAAS).

b. Platform as a Service (PAAS): With PAAS, the cloud provider supplies not just the hardware but also a toolkit and a range of supported programming languages for creating higher level services, or software programs that are made accessible as a component of a particular platform (Chen & Zhao, 2021). Usually, software developers who host their apps on the platform and make them available to end users are the PAAS users. Developers can launch their apps on the cloud with PAAS. Although they have no control over the underlying infrastructure, consumers do have power over the applications they use. Through the internet, it gives users access to a comprehensive suite of software. Platform as a Service (PAAS) computer platform delivery include; Salesforce Platform, Microsoft Azure, Amazon Web Services, and Google App Engine are a few PAAS examples.

c. Infrastructure as a Service (IAAS): Users can access resources including servers, storage, networks, and data center space by using IAAS. It distributes the pool of computational power. On IAAS, users can install and operate operating systems and applications. It spares the user from having to purchase or maintain underlying hardware and software. Amazon EC2 is a fantastic illustration of IAAS (Cloud Evolution, 2023).

Services offered by cloud computing are economical, adaptable, and efficient. This system isn't completely safe, though. Regarding cloud computing, security and privacy are the main issues. The cloud computing industry has a number of security problems. Data security appears to be the

main barrier preventing cloud computing from being used, out of all the security concerns. Using a shared public cloud securely is more difficult than using a private cloud. Public clouds are better suited for incidental or less vulnerable applications because of this (Jamil & Zaki, 2021).

II. REVIEW OF RELATED WORK

Numerous studies in cloud computing and cloud security have been conducted to create a safe environment for effective operations. In order to prevent unwanted access and guarantee data confidentiality, integrity, and availability, storage providers should address the legal and regulatory issues related to security concerns, encryption schema, scheduled data backups, and stringent access control mechanisms (Han & Susilo, 2023).

An identity-based proxy re-encryption system was presented in a related study to transfer sensitive data from the owner to a third party. This technique is appropriate for cloud computing scenarios since it supports both intra-domain and inter-domain queries. The access key in the suggested method is connected to the requested cipher text as well as the requester's identity and can be independently computed by the owner without the use of a private key generator (PKG) (Kaufman, 2019). Although this scheme is similarly protected from collusion assaults, recent malware attacks have caused some setbacks.

A searchable encryption system is another innovation from the Microsoft Cryptography Group (Kamara & Lauter, 2020). A local program that is installed on the user's computer and consists of three modules; a data processor, a data verified, and a token generator which is the foundation of this system's operation. Prior to transferring the data to the cloud, the user encrypts it. The

user generates a token and a decryption key using the token generator whenever some data is needed.

The chosen file or files are downloaded, the token is sent to the cloud, the files are checked locally, and the key is used to decrypt them. Sending the token and decryption key to a different user you wish to work with allows sharing. To make the collaboration process simpler, the corporate version of the system adds a credential generator; nevertheless, the researchers' approach differs from the suggested approach utilized in this study.

There has been a proposal for a system that can effectively safeguard data from start to finish, meaning from the owner to the cloud and finally to the user (Sood, 2022). The data protection strategy makes use of a number of cryptographic techniques, including the division of data into three distinct sections for storage in the cloud, searchable encryption, Secure Socket Layer (SSL) 128 bit or 256 bit encryption, and Message Authentication Code (MAC) for data integrity checks. Although the proposed approach provides some degree of Confidentiality, Integrity, and Availability (CIA), it is unable to ensure the security of data from a device owned by a third party.

III. DATA SECURITY ISSUES IN CLOUD

To be sure that no unauthorized individual has accessed the data, cloud data security is required. Because the needs of the security audience are distinct, the data security lifecycle differs from information lifecycle management. The six stages of the lifespan, which go from creation to destruction, specify that while data is depicted as progressing linearly, once it is produced, it can

move freely between them and might not go through them all (Data Security lifespan 8.0, 2024). The data flow order is shown in Figure 1.

- Create: This is the process of creating new digital content or updating or changing already-existing content.
- Store: The process of committing digital data to a storage repository usually happens almost concurrently with creation.
- Use: Information is seen, processed, or utilized in different ways during an activity.
- Share: Information is shared amongst users, clients, and partners.
- Data that is archived is taken out of use and kept for a long time.
- Destroy: Using physical or digital methods (such as crypto-shredding), data is permanently deleted.

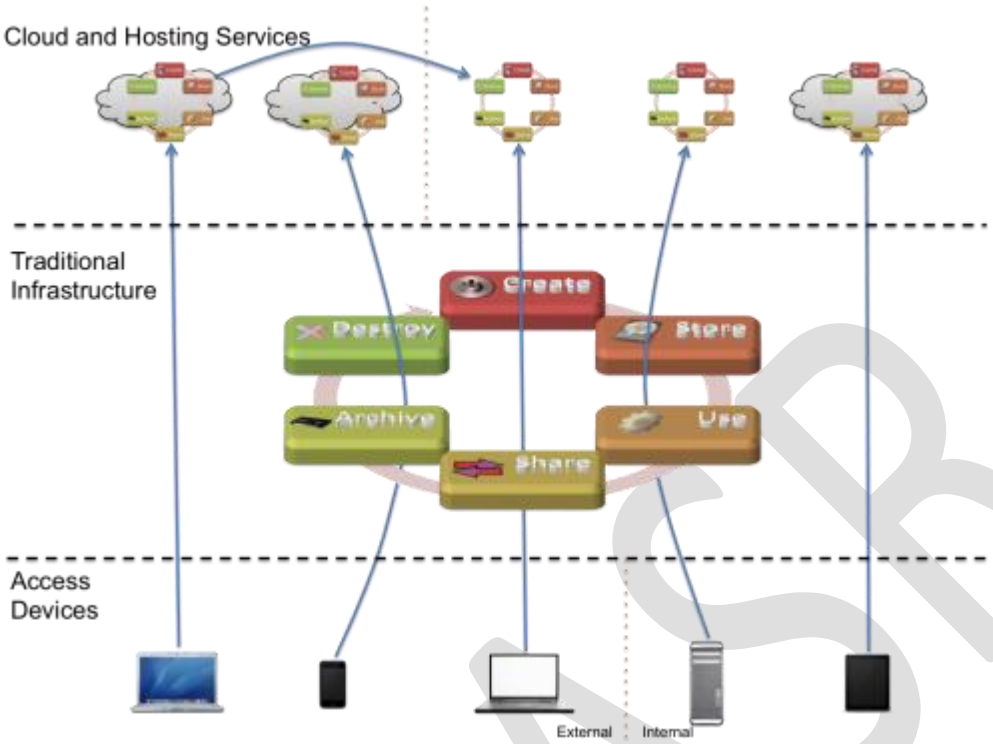


Fig. 1: Cloud Access Devices (Data Security Lifecycle, 2024)

Although it doesn't address where information is stored or how it is accessed, the lifecycle depicts the stages it goes through. To demonstrate this, consider the Lifecycle as a collection of smaller lifecycles that are executed in various operating conditions rather than as a single, linear operation. Data can flow into, out of, and between these settings at almost any stage. Recognizing these movements and implementing the appropriate controls at the appropriate security boundaries are crucial to data security. These sites can be internal, external, public, private, hybrid, and so on, much like with cloud deployment patterns. others might be typical outsourcers, others might be cloud providers, or there might be several sites inside one data center (Liu, 2022).

There are currently six concepts to comprehend regarding data security: Where may the data possibly be located? What controls and lifecycles exist in each of those places? Where may data flow between places during each lifecycle? What channel does data use to travel between locations? By whom is the data accessed? And with what device and channel can one access it? Access to data is possible today through a wide variety of devices. With a few notable exceptions, the days of employees only having access to data through restricted apps on locked-down workstations are rapidly coming to an end. These devices may run different apps and have different security features. In particular, we've moved several applications to SAAS suppliers, who frequently create unique mobile applications with features not found in PCs. With several data locations (and application environments), each with a unique data lifecycle, and all accessible by a range of devices in various places, Figure 1 illustrates how complicated this may get. While some data is stored in one place and never leaves, other data flows between different locations and occasionally even between external sources (Liu, 2022).

Since the cloud architecture is spread, there must be more data transits across networks, which presents new and difficult security risks. Whether data is in transit (to and from the cloud) or at rest (i.e., kept in the cloud), confidentiality must be guaranteed. It would be ideal to offer a closed execution environment where the owner could confirm the data's confidentiality and integrity. Although encryption offers a secure way to store data on the cloud, cloud-based processing does not work well with it (Mahmood, 2021). This latter issue arises because, in most cases, data is stored in the cloud and used by cloud-based apps. The majority of the time, when data is stored on the cloud, encryption is required. Moreover, doing computations with encrypted

data would require more computing resources, which would result in higher costs. Some operations would simply not be able to complete with encrypted data.

There have been recent initiatives to address this problem. The first is the Trusted Cloud Computing Platform, which seeks to implement the cloud version of the Trusted Computing concept (NIST, 2023). Nonetheless, the goal of this project is to safeguard the cloud service company from malevolent insiders.

IV. MATERIALS AND METHODS

The components of the proposed cloud based security system include; MySQL, Java EE 21, Web server, Websocket, Apache Netbeans 21. The proposed system was built using Unified Modelling Language (UML) that integrates the above listed components for an efficient and secured chat platform built around the cybersecurity goal of CIA. The Use Case presentation, which graphically illustrates the interactions between the system, the external system, and the user, as well as the individual components of the system and how they interact with other software components, how the system will operate, and how entities interact with other (components and interfaces), are some of the diagrammatical elements that can be visualized with the help of the UML. Use case diagrams are essential to system design because they serve as a guide for building the system's structure and specify who will use it and how they anticipate to interact with it. Figure 2 shows the proposed cloud base security system workflow diagram of the chat group collaborating system for a secured information dissemination between the cloud and the user. The system is made up of an enhanced encrypted cloud services built with the materials described in this session. Figure 3a represents the Admin Use case Diagram, Figure 3b

is the user Use Case diagram while Figure 4 depicts a simple class diagram representing the system all embedded with private and public key as well as authentication functions.

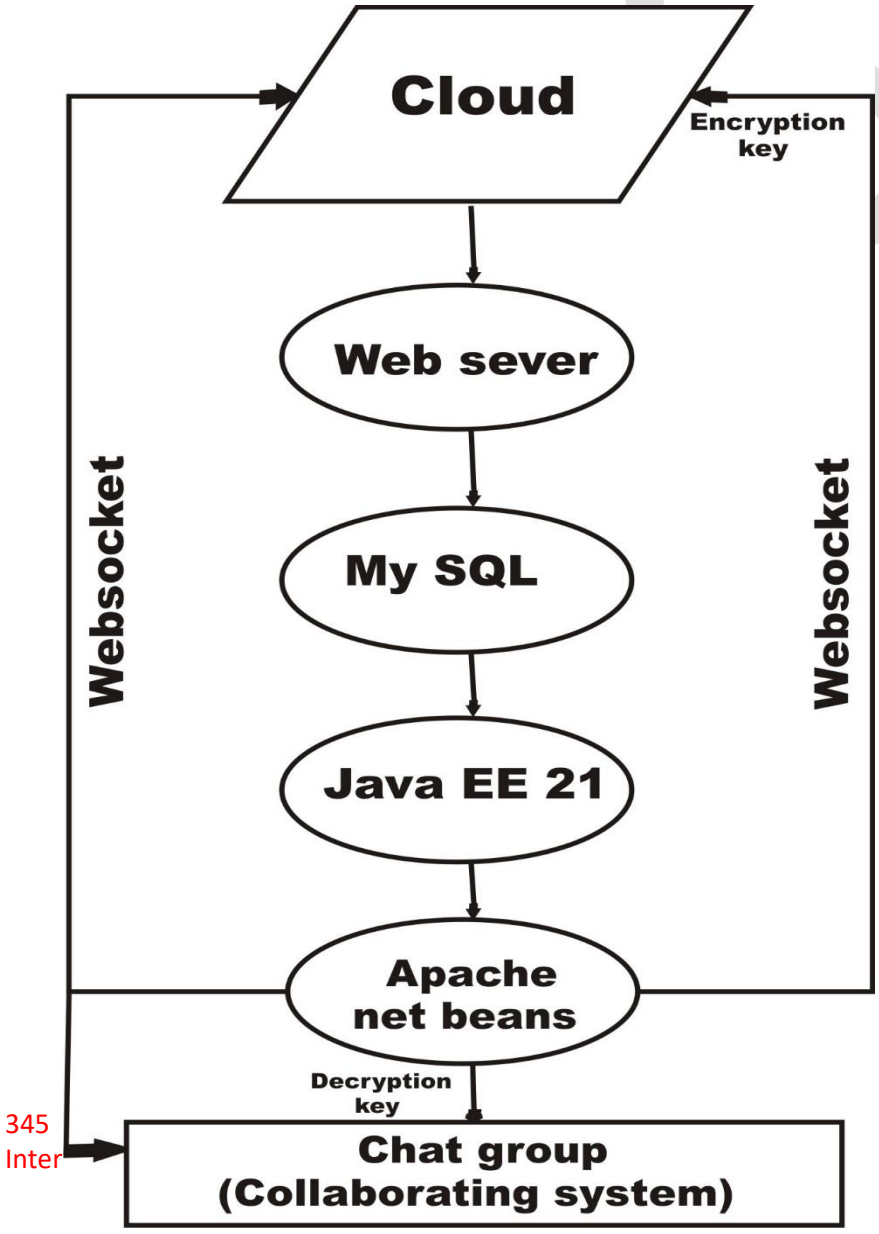
A. Java EE 21**:** This is a Java programming language that is object-oriented, similar to Oracle's enterprise Java computing platform. For the purpose of creating and executing enterprise software, such as network and web services as well as other sizable, multi-tiered, scalable, dependable, and secure network applications, the platform offers an API and runtime environment.

B. WebSocket: Using a single TCP connection, this protocol offers full-duplex communication channels. The WebSocket API in Web IDL has been defined by the W3C, whereas the WebSocket protocol was standardized by the IETF as RFC 6455 in 2011. WebSocket can be used by any client or server application, however it is intended to be implemented in web browsers and web servers.

C. MySQL Relational Database: In the corporate world, databases are typically used to automate bookkeeping, employee information, and invoicing. In addition, business databases are utilized to monitor billing, inventory, and shipping. Businesses may easily find documents thanks to a database's search capabilities and generate summaries with ease thanks to its report features. Additionally, databases enable companies to repurpose their current data.

D. Webserver: The task of the web server appears to be quite simple. Operating on top of the operating system, it simply sits there, waiting for any requests that users may make on the Internet. It then replies to those requests and displays the relevant web pages.

E. Apache Netbeans 21: This is one of the tools among other tools used by java developers. Other developing tools include JCreator, JBuilder, JEclipse etc. We relied on the Netbeans tool as a very handy tool in building graphical user interface programs. Netbeans 21 is a new netbeans with an enhanced features making complex programming easier. Our NetBeans is built on java standard edition technology and cannot be used without the java Standard Edition Development Kit, this setup is downloadable from the sun Microsystems official website www.java.sun.com.



345
Inter

Fig. 2: System Workflow

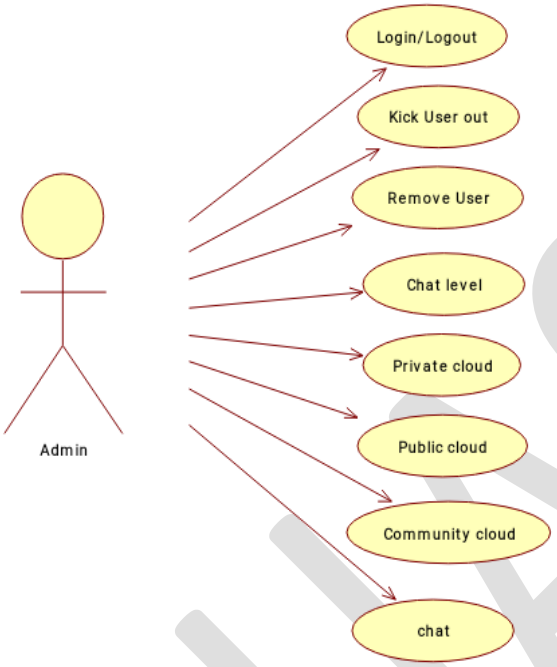


Fig. 3a: Use case diagram for admin

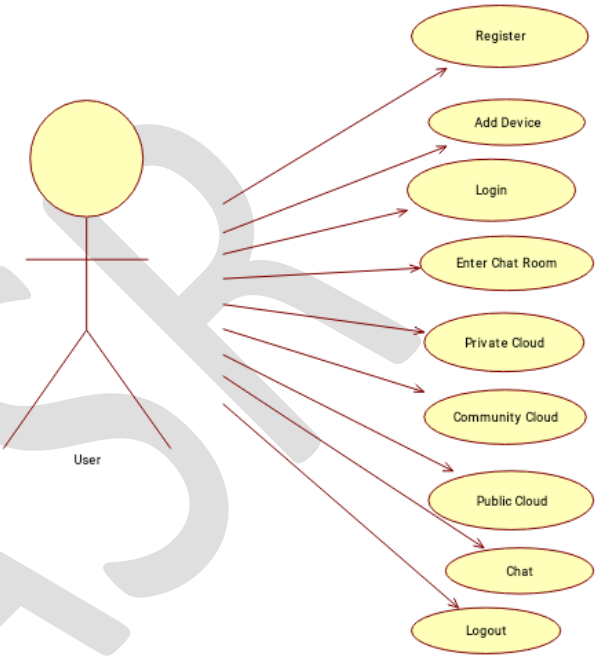


Fig. 3b: Use case diagram for users

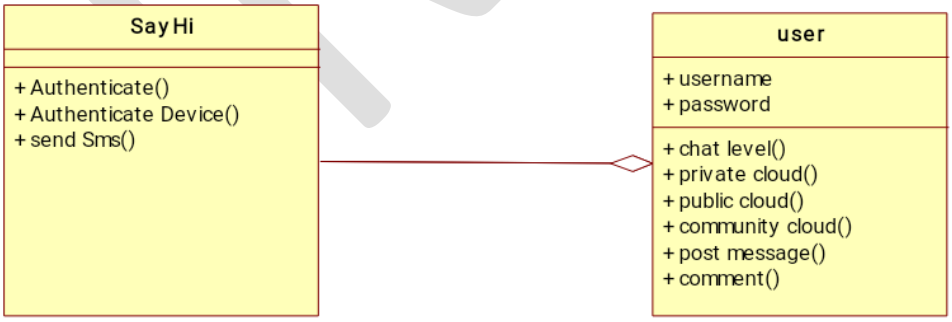


Figure 4: class diagram representing the system

V. RESULTS AND ANALYSIS

We developed a chat application with high security posture at both the server and user ends where users can communicate through text web based live chat, as well as a database for the system, to ensure that there is no unauthorized access to network resource and to ensure that the IP address of the user is authenticated to prevent unauthorized access.

The proposed system is built in such a way that users could create and secure their account, add device, login, select chat room, post, view messages and chat/collaborate with each other. Figure 5a, 5b and 5c display the add device, login and chat room interfaces of the system.

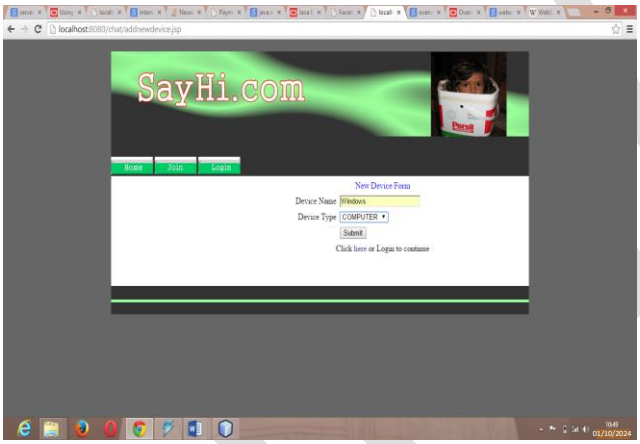


Fig. 5a: Add device interface

Figure 5b: Login interface

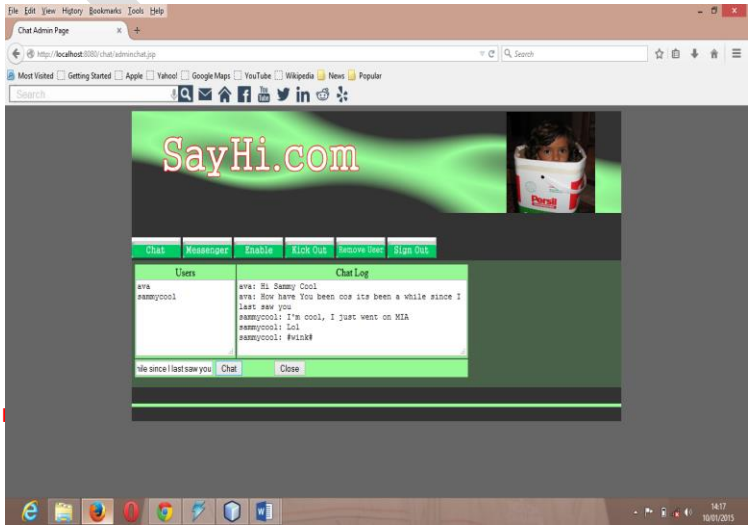


Fig. 5c: Chat Room

The add device interface collects the information about the user's system which is used for the registration as a way to secure his/her account from unauthorized user as seen in Figure 5a. The user then complete the login process to gain access to system's resource that requires authorization as shown in Figure 5b. In this interface, the user is required his/her username and password, if a wrong username or password is entered, access to the system is denied. Whereas, the chat room interface, provides the avenue for a user to select the room of his/her interest where he/she can post message or post comment on other user's message or chat with other users online. Some of the security features embedded in this system include but not limited to; encryption key, cryptography (private and public key) for authentication.

VI. CONCLUSION

A revolutionary new method of information delivery is cloud computing. It is transforming delivery patterns, empowering businesses to re-engineer their business processes, make incremental improvements in IT agility, and completely transform how they utilize apps and communicate with customers and other businesses. Cloud computing is based on a whole new understanding of computing that much more directly links IT to business value. Cloud makes it evident that the information stored in the hardware is what gives a data center its value, not the stacks of hardware and networks that comprise it. Since information is precious, it must be both safe and easily accessible. In this study, we have developed a cloud based chat platform where

information could be transferred among group of users in real-time at the same maintaining a high level of security.

The use of UMI tools such as activity diagram, class diagram and use case has made our work unique as we successfully integrate the system components. We strongly recommend that organization adopt this system to aid efficient communication and collaboration among staff in a secured environment.

REFERENCES

Armbrust, M., Fox, A., Grith, R., Joseph D, A., R, K., Konwinski, A., Zaharia, M. (2010). A view of Cloud Computing. *Communication of the ACM Vol. 53, No. 4*, 50-58.

Buyyaa, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2020). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 3-18.

Chen, D. & Zhao, H. (2021). Data Security and Privacy Protection Issues in Cloud Computing. *International Conference on Computer Science and Electronics Engineering Vol. 1* , pp. 647-651.

Data Security Lifecycle 8.0. (2024). Retrieved July 21, 2024, from Securosis: https://www.securosis.com/blog/data-security-lifecycle-8.0

Evolution of cloud: Interactive infography. (2023). Retrieved July 19, 2024, from Symantec: http://www.emea.symantec.com/web/evolutiontocloud/

Han, J. & Susilo, W. (2023). Identity-based data storage in cloud computing. Future Generation Computer Systems, vol. 29, no. 3, 673–681.

Jamil, D. & Zaki, H. (2021). Cloud Computing Security. International Journal of Engineering Science and Technology, Vol. 3, No. 4, 3478-3483.

Kamara, S. & Lauter, K. (2020). Cryptography Cloud Sorage. Microsoft Research Cryptographic Group, 19-20.

Kaufman, M. (2019). ‘‘Data security in the world of cloud computing’’. *Security & Privacy, IEEE, vol. 7*, 61–64.

Liu, W. (2022). Research on cloud computing security problem and strategy. *in Consumer Electronics, Communications and Networks (CECNet), 2022 2nd International Conference on*, 2216–2219.

Mahmood, Z. (2021). Data location and security issues in cloud computing. *in Emerging Intelligent Data and Web Technologies (EIDWT), 2021 International Conference* , pp. 49–54.

NIST (2023). Cloud Computing Program. Retrieved July 20, 2024, from NIST Information Technology Laboratory: http://www.nist.gov/itl/cloud/

Sood, K. (2022). A combined approach to ensure data security in cloud computing. *Journal of Network and Computer Applications, vol. 35, no. 6*, pp. 1831–1838.