Mambilla Journal of Science and the Environment Vol. 10, Issue 1, Page No. 36-40

MAMBILLA JOURNAL OF SCIENCE AND THE ENVIRONMENT

journal homepage: https://oer.tsuniversity.edu.ng/index.php/mjse

A SOFTWARE FRAMEWORK FOR SECURE CLOUD FILE HOSTING USING AN IOT-BASED SECURITY APPROACH

[1*]Shallom, S., [2]Malgwi, Y.M.

[1]Department of Computer Science, Taraba State University, Jalingo, Nigeria.
[2] Department of Computer Science, Modibbo Adama University, Yola, Nigeria.

ARTICLE INFO

Article history:
Received 02 December 2025
Received in revised form 19 January 2026
Accepted 20 January, 2026

Keywords:
Cloud file hosting, Internet of Things, security framework, access control, encryption.

ABSTRACT

Cloud file hosting platforms have become essential for data storage, collaboration, and information sharing in modern institutions. Despite their benefits, traditional cloud systems face persistent security challenges, especially when integrated with Internet of Things (IoT) devices that generate and access sensitive data. These challenges are more pronounced in developing regions, where infrastructural constraints and evolving regulatory frameworks complicate secure cloud adoption. This paper presents the design of a software framework for a robust cloud-based file hosting platform that integrates IoT-based security mechanisms to enhance data confidentiality, access control, and system resilience. The proposed framework adopts a modular architecture that incorporates IoT-aware authentication, role-based access control, multi-layer encryption, and secure cloud storage services. Using a design science research methodology, the framework is conceptually developed and analyzed to demonstrate how IoT security components can be embedded into cloud file hosting without the need for costly full-scale system deployment. The framework is evaluated conceptually based on performance, security robustness, and the ability to be deployed within academic institutions in Nigeria. The findings indicate that a framework-based approach provides a scalable, cost-effective, and adaptable solution for secure cloud file hosting in resource-constrained environments.

1. Introduction

Cloud computing has transformed the way organizations store, manage, and share digital information by providing scalable resources, reduced infrastructure costs, and global accessibility (Mell & Grance, 2011; Armbrust *et al.*, 2010). Cloud file hosting platforms such as Google Drive, Dropbox, and OneDrive are widely adopted in academic and enterprise environments due to their flexibility and collaborative features. However, the increasing integration of cloud services with Internet of Things (IoT) devices has introduced new security and privacy concerns (Ari *et al.*, 2019; Stergiou *et al.*, 2021).

IoT devices generate large volumes of data and often operate with limited computational and security capabilities, making them attractive targets for cyber-attacks (Alwarafy *et al.*, 2020). When IoT-generated data is stored or processed in cloud environments, vulnerabilities related to authentication, access control, encryption, and data integrity become more critical (Karati *et al.*, 2021). These issues are particularly challenging in developing countries such as Nigeria, where intermittent internet connectivity, limited technical resources, and evolving data protection regulations affect secure cloud adoption (Okoye *et al.*, 2014; Alabi, 2018).

Existing research has largely focused on isolated security techniques, such as encryption algorithms or access control models, without providing a unified and reusable framework that integrates IoT security with cloud file hosting (Mittal, 2017; Bisalapur *et al.*, 2020). Moreover, many proposed solutions are prototype systems that are difficult to deploy or scale in real institutional environments. This paper addresses this gap by proposing a software framework that integrates IoT-based security mechanisms into cloud file hosting platforms, with a focus on academic institutions in developing regions.

* Corresponding author: +2348065845630
E-mail address: satishallom@gmail.com

Research on cloud file hosting security has identified major challenges including unauthorized access, data leakage, and multi-tenancy risks (Tawalbeh *et al.,* 2020; Veerasingam *et al.,* 2023). Encryption-based approaches, particularly hybrid cryptographic schemes, are commonly proposed to protect cloud data (Bisalapur *et al.,* 2020; Gwande & Selvam, 2023). While effective, these approaches often overlook IoT-specific threats.

2. Review of Related Literature

2.1 Cloud File Hosting and Security Challenges

Cloud file hosting systems have become widely adopted due to their ability to provide scalable storage, remote access, and cost-effective data management. These systems allow users to upload, store, and retrieve files from anywhere through Internet-based platforms. Despite these advantages, security remains a major concern, particularly in relation to data confidentiality, integrity, and availability. Veerasingam *et al.*(2023) note that cloud environments are frequent targets of cyberattacks due to the concentration of sensitive data on shared infrastructures. In multi-tenant cloud architectures, multiple users and organizations share the same physical resources, which increase the risk of data leakage, privilege escalation, and unauthorized access if isolation mechanisms are weak. Tawalbeh *et al.*(2020) further emphasize that threats such as insider attacks, misconfigured access controls, and insecure APIs continue to undermine trust in cloud file hosting platforms. These challenges highlight the need for stronger security frameworks that go beyond traditional authentication and incorporate layered protection mechanisms.

2.2 Internet of Things and Cloud Integration

The integration of the Internet of Things with cloud computing, commonly referred to as the Cloud of Things, has enabled efficient collection, storage, and analysis of large volumes of sensor-generated data. IoT devices continuously generate data that is transmitted to cloud platforms for processing and long-term storage, supporting applications in smart campuses, healthcare, and industrial systems (Ari *et al.,* 2019). However, this convergence significantly expands the attack surface of cloud environments. Kumar and Sharma (2023) explain that many IoT devices are resource-constrained, lacking sufficient processing power and memory to support advanced security mechanisms. As a result, they often rely on weak authentication methods, making them vulnerable to device impersonation, spoofing, and unauthorized access. Karati *et al.*(2021) argue that without proper IoT-aware security integration, compromised devices can serve as entry points for attackers to access cloud-stored data. These issues underscore the importance of designing cloud frameworks that explicitly incorporate IoT-based authentication and monitoring to ensure secure interaction between devices and cloud services.

2.3 Access Control Mechanisms

Access control is a critical component of cloud security, as it determines who can access specific data and system resources. Role-Based Access Control (RBAC) assigns permissions based on predefined user roles, such as administrator, staff, or student, making it simple and efficient for managing large user groups (Jayant *et al.*, 2015). Attribute-Based Access Control (ABAC), on the other hand, provides finer-grained control by considering multiple attributes such as user identity, resource type, and environmental conditions (Mittal, 2017). While both models are widely used in cloud systems, most existing implementations focus primarily on user attributes and ignore the context of the accessing device. Karati *et al.* (2021) highlight that access decisions rarely consider IoT device trust levels, firmware status, or device location. This limitation creates security gaps, especially in IoT-enabled environments where compromised or untrusted devices may still gain access to sensitive cloud resources. Therefore, integrating device-aware access control into cloud frameworks is essential for improving overall system security.

2.4 Encryption Techniques in Cloud Systems

Encryption plays a central role in protecting data stored and transmitted within cloud environments. To balance security and performance, many cloud systems adopt hybrid encryption schemes that combine symmetric algorithms such as AES for fast data encryption with asymmetric algorithms such as RSA for secure key exchange (Bisalapur *et al.,* 2020). Gwande and Selvam (2023) report that hybrid encryption significantly reduces computational overhead while maintaining strong security guarantees. Beyond hybrid encryption, recent studies emphasize the importance of multi-layer encryption strategies. These approaches apply encryption at multiple stages, including data at rest in storage, data in transit over networks, and data during processing within applications (Liu *et al.,* 2021). By securing data across all lifecycle stages, multi-layer encryption minimizes exposure even if one security layer is compromised. However, effective key management and integration with authentication mechanisms remain challenges, particularly in IoT-enabled cloud systems, reinforcing the need for well-structured security frameworks.

3. Methodology

3.1 Research Design

This study adopts the Design Science Research Methodology (DSRM), which is suitable for developing and evaluating IT artifacts such as software frameworks (Peffers *et al.*, 2007).

3.2 Framework Architecture

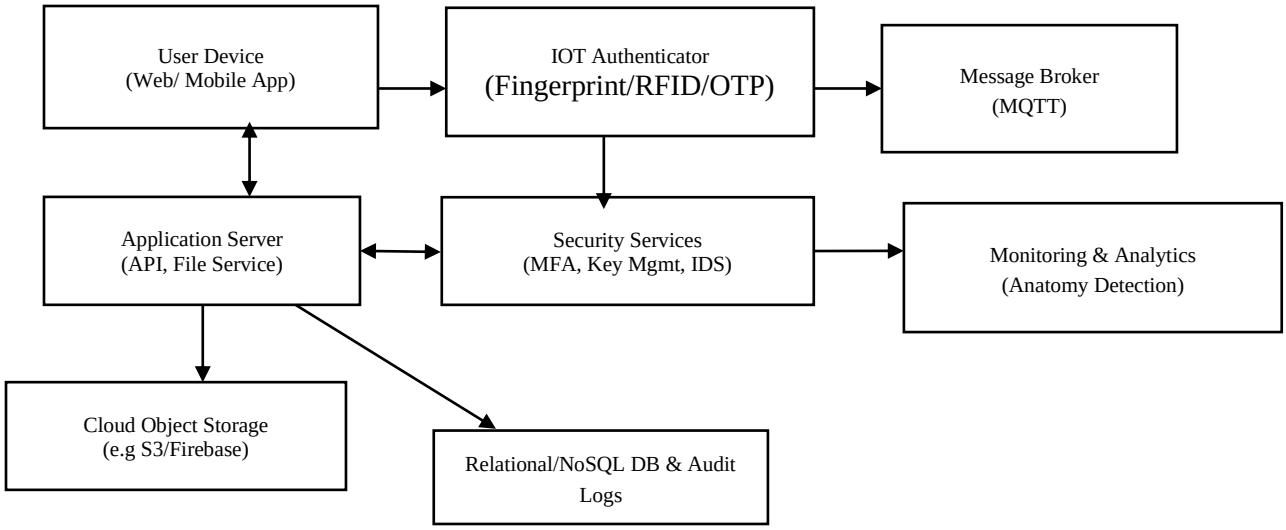

Figure 1: Framework Architecture

Figure 1 presents the architecture of the IoT-secured cloud file hosting framework. The framework follows a layered design to ensure modularity, scalability, and security. User interactions occur through the user interface layer, which forwards requests to the application layer for authentication, authorization, and file management. IoT-based security is enforced through a dedicated IoT security layer that validates device codes generated by trusted IoT devices. Encryption and key management are handled by the security services layer before data is stored in cloud storage. This modular architecture supports secure file hosting while remaining adaptable to institutional environments.

3.3 Framework Operational Flow

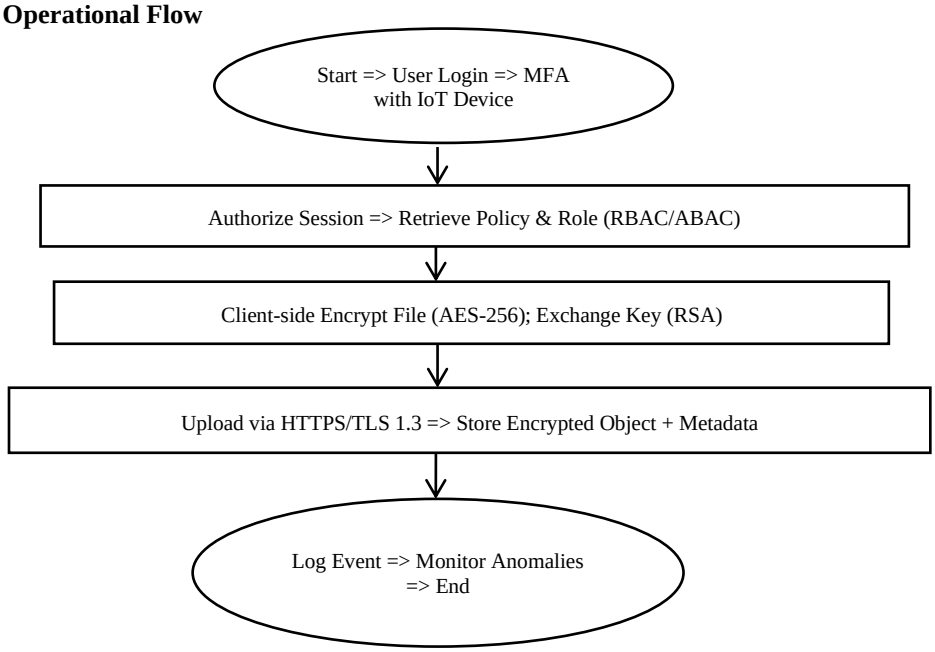

Figure 2: Framework Operational Flow

Figure 2 illustrates the operational flow of the proposed framework during secure file access and storage. Authentication begins with user credentials and an IoT-generated device code. Upon successful validation, role-based access control determines authorization rights. Files are encrypted before storage or transmission to ensure confidentiality. System activities are logged to support auditing and intrusion detection. This flow demonstrates how the framework enforces security at multiple stages of interaction.

4. Results and Discussion

The proposed framework demonstrates how IoT-aware authentication improves security by validating both user credentials and trusted devices. Multi-layer encryption ensures end-to-end data protection, while modular design supports scalability and adaptability. Compared to standalone systems, the framework approach reduces development cost and supports gradual institutional adoption. These results align with findings by Stergiou *et al.* (2021) and Alwarafy *et al.* (2020), which emphasize integrated security architectures for cloud-IoT systems.

The results demonstrate that the framework successfully integrates IoT-based authentication, access control, encryption, and monitoring into a cohesive cloud file hosting solution. The modular design allows each security component to operate independently while contributing to overall system robustness. Compared to conventional cloud file hosting platforms that rely mainly on single-factor authentication, the proposed framework provides stronger protection against unauthorized access and data breaches.

Conclusion

This paper presents a software framework for secure cloud file hosting that integrates IoT-based security mechanisms. The framework addresses key security challenges by combining IoT-aware authentication, access control, and encryption within a reusable and deployable architecture. From a practical perspective, the framework's interface-level implementation confirms its feasibility for academic institutions, particularly in environments with limited resources. The results indicate that a framework-based approach can achieve secure and reliable file hosting without the cost and complexity of deploying a fully standalone system. Future work will focus on pilot deployment and empirical performance evaluation.

References

Alabi, A. (2018). Cloud computing adoption in Nigeria: Issues and challenges. *International Journal of Cloud Applications and Computing. (Include volume and page numbers if available)*

Alwarafy, A., Al-Thelaya, K. A., Abdallah, M., Schneider, J., & Hamdi, M. (2020). A survey on security and privacy issues in edge computing-assisted Internet of Things. *IEEE Internet of Things Journal.*

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM, 53*(4), 50-58.

Ari, I., Sasikumar, P., & Suganthi, A. (2019). Cloud of Things: Architecture and security issues. *International Journal of Engineering and Advanced Technology. (Add volume/page)*

Bisalapur, S., Patil, M., & Hugar, S. (2020). Hybrid cryptographic algorithms for cloud security. *Journal of Cloud Computing, 9*(1), 1–15.

Gwande, J., & Selvam, G. (2023). File storage system using hybrid cryptography in cloud computing. *International Journal of Advanced Research in Science, Communication and Technology, 3*(5). http://dx.doi.org/10.48175/IJARSCT-11643

Jayant, R., Patel, A., & Thakkar, H. (2015). Enhanced RBAC model for cloud storage. *International Journal of Engineering and Technology*.

Karati, A., Islam, S. H., Karuppiah, M., & Amin, R. (2021). Provably secure and lightweight authentication protocol for IoT-based cloud environment. *IEEE Internet of Things Journal, 8*(7), 5390-5403.

Kumar, S., & Sharma, P. (2023). Edge-enabled cloud of things security frameworks. *Journal of Network and Computer Applications, 215*, 103580.

Liu, X., Wang, Y., & Chen, H. (2021). Multi-layered encryption for cloud data protection. *IEEE Transactions on Cloud Computing, 9*(2), 314–326.

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing* (Special Publication 800-145). National Institute of Standards and Technology.

Mittal, S. (2017). Attribute-based encryption for secure cloud file sharing. *International Journal of Security and Its Applications, 11*(5), 1-12.

Okoye, J., Obodoeze, F., & Asogwa, T. (2014). Cloud adoption in Nigeria: Security and regulatory challenges. *African Journal of Information Systems, 6*(2), 1-13.

Stergiou, C., Psannis, K., & Kim, B. (2021). Cloud of things security challenges and directions. *Future Internet, 13*(6), 142.

Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT privacy and security: Challenges and solutions. *Applied Sciences, 10*(12), 4102. https://doi.org/10.3390/app10124102

Veerasingam, S., Jayaraj, R., & Joseph, A. (2023). Security in public cloud storage: A systematic review. *Journal of Cloud Computing, 12*(10), 1-23.