HINWEIS Research

# Develop a High Storage Cloud Platform that Provides Enhanced Security

Harshal Prabhakar Gavali (RIT, Islampur)
Adharva Kumar Thodupunooru (RIT, Islampur)

# Introduction

- Emphasis on security and privacy in cloud storage dynamics.
- Explores one-to-many encryption, data integrity, resilient data deletion, and privacy solutions.
- Integrates RSA, AES, homomorphic, and searchable encryption for robust cloud defense.
- Uniquely integrates GitHub load balancer for efficient data management and balanced distribution.
- Committed to evolving encryption tech with future research aligned to identified security needs in cloud storage.

# Background of the Paper

- Enhancement of data security and privacy in cloud storage.
- One-to-many encryption, data integrity, resilient data deletion, and privacy-preserving solutions.
- Leveraging technologies like AES, RSA, and searchable encryption.
- Integration of load balancing for efficient data distribution.
- Development environment setup, encryption (RSA and AES), security measures, GitHub integration.

# Related works

- Previous Studies: Extensively explored encryption methodologies such as Identity-Based Encryption (IBE), Attribute-Based Encryption (ABE), homomorphic encryption, and searchable encryption.
- Previous works have addressed storage management approaches in cloud environments.
- Previous studies have recognized the imperative to fortify security measures against emerging threats, especially in the domain of post-quantum encryption.

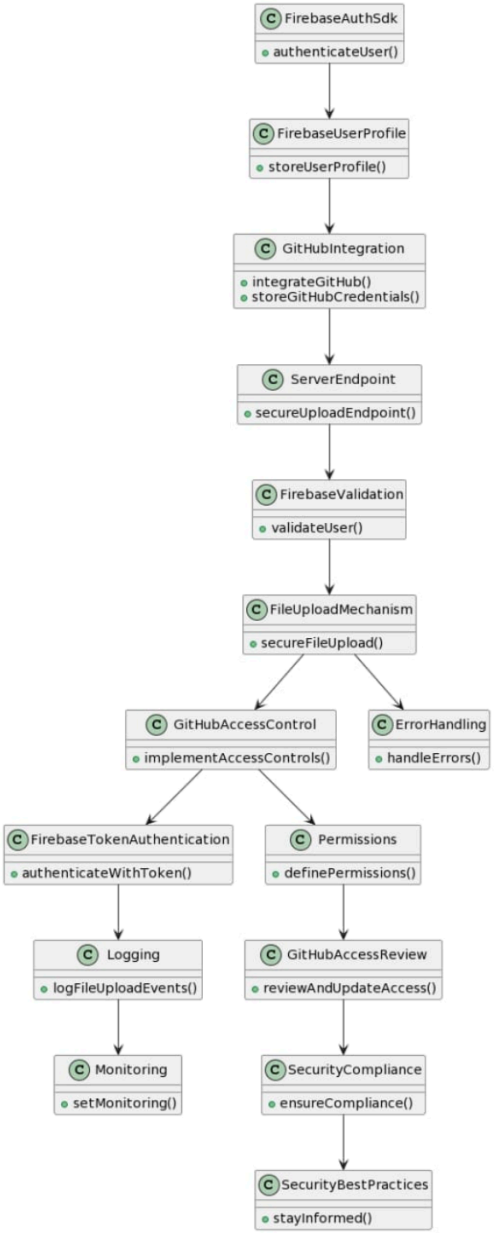
# Problem Formulation

- With the continuous evolution of cloud storage, integrating cutting-edge technologies poses challenges in terms of seamless functionality and security.
- Conventional storage management approaches may not fully optimize resource utilization and ensure balanced data distribution for a single user.
- As data volumes and user demands grow, scalability challenges may emerge, and the system may need to be future-proofed against evolving threats.

# Proposed System

- Implement advanced encryption methodologies like RSA, AES, homomorphic encryption, and searchable encryption for robust data security.
- Incorporate a load balancer with GitHub to optimize resource utilization and achieve balanced data distribution for a single user across multiple repositories.
- Implement a comprehensive methodology for developing a secure cloud storage platform, covering risk assessment, security implementation, user authentication, data encryption, access control, and monitoring.

# Proposed System



# Results

- Through rigorous experimentation and simulation using competent machines, the results demonstrated the robustness of the encryption system in safeguarding user data against potential security breaches.
- Experimentation in relevant conditions showcased optimized resource utilization, balanced data distribution, and enhanced operational efficiency, validating the effectiveness of the load balancing approach.

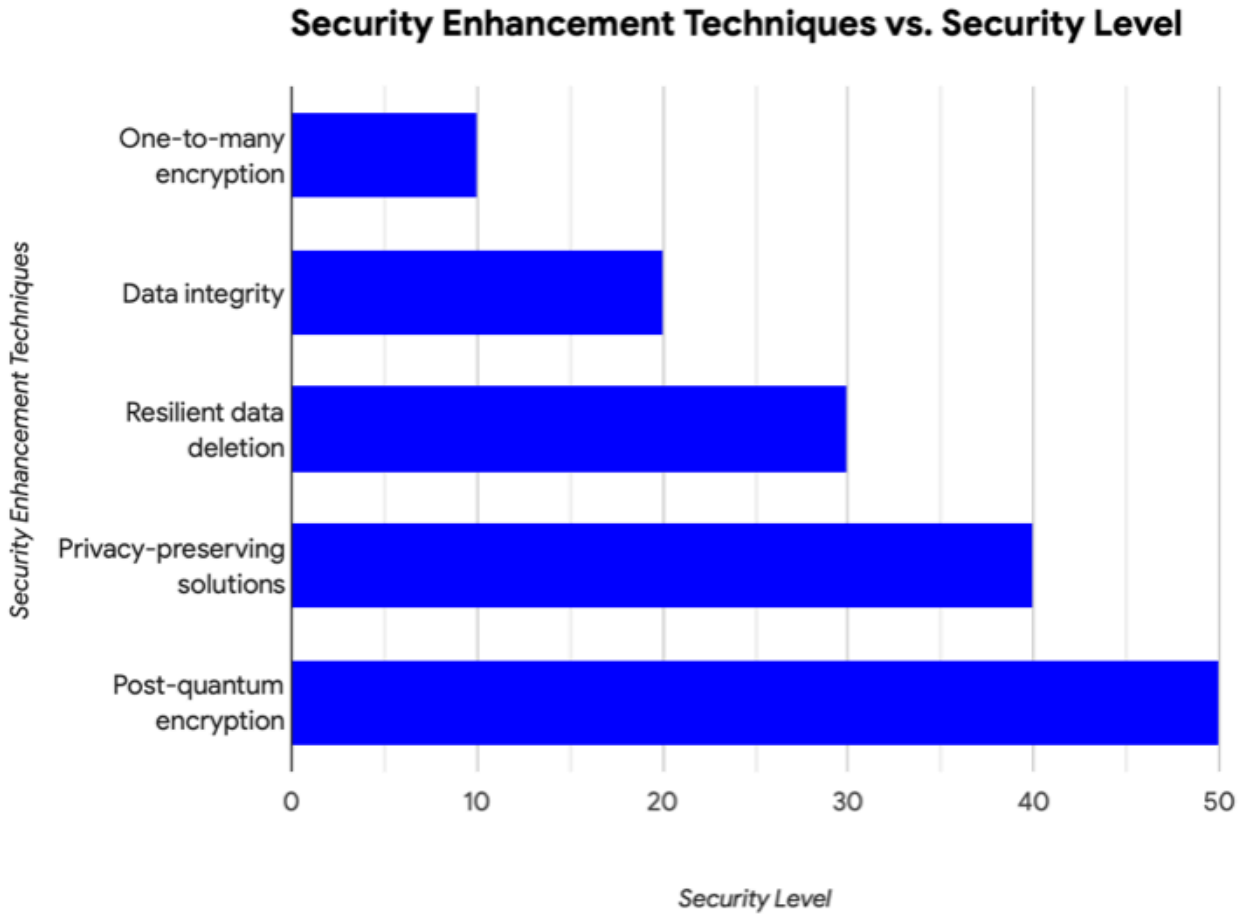
# Results

- The system's performance was evaluated through relevant conditions, and the results highlighted the success of the methodology in providing a systematic and secure approach to cloud storage platform development.

# Comparison

- Conduct a comprehensive study on the confidentiality, integrity, and accessibility of user data under various scenarios. Compare encryption strengths and vulnerabilities.
- Analyze the distribution of data across multiple repositories for a single user, assessing the impact on operational efficiency and potential vulnerabilities.

# Comparison



# Discussion

- Diverse encryption methods, such as RSA, AES, homomorphic, and searchable encryption, effectively bolstered data security in cloud storage.
- Integrating a load balancer with GitHub optimized resource utilization, distributed data storage, and enhanced overall system security in cloud storage.
- Recognition of the need for post-quantum encryption emphasizes the ongoing importance of resilient encryption techniques against emerging quantum threats in the cybersecurity landscape.

# Conclusions

- The research significantly enhances cloud storage security through various encryption methodologies, including RSA, AES, homomorphic, and searchable encryption.
- Integration of a load balancer with GitHub optimizes resource utilization, ensuring balanced data distribution, thereby enhancing security and operational efficiency.
- The exploration of post-quantum encryption reflects a forward-looking commitment to staying ahead of emerging threats, emphasizing the continuous need for exploration in data encryption technologies.

# Future work

- Proactively fortify the system against evolving cybersecurity challenges, with a specific emphasis on quantum-resistant algorithms.
- Investigate dynamic load balancing mechanisms capable of adapting to varying workloads, prioritizing critical tasks in real-time for improved efficiency.
- Conduct real-world implementations and comprehensive testing to evaluate practical performance, usability, and scalability in varied cloud storage environments.

# References


[1] Yang, Pan, Naixue Xiong, and Jingli Ren. "Data security and privacy protection for cloud storage: A survey." IEEE Access 8 (2020): 131723-131740.

[2] Yu, Jia, et al. "Enabling cloud storage auditing with key-exposure resistance." IEEE Transactions on Information forensics and security 10.6 (2015): 1167-1179.

[3] Ren, Kui, et al. "Secure and efficient data retrieval over encrypted cloud storage using CP-ABE with constant-size ciphertexts." IEEE Transactions on Information Forensics and Security 9.11 (2014): 1853-1864.

[4] Wang, Qian, et al. "Towards achieving revocable and fine-grained access control in cloud computing." IEEE Transactions on Information Forensics and Security 9.11 (2014): 1922-1933.

[5] Li, Ming, et al. "Efficient fine-grained access control in cloud storage." IEEE Transactions on Cloud Computing 7.2 (2019): 581-593.