KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY
KUMASI

COLLEGE OF SCIENCE
DEPARTMENT OF COMPUTER SCIENCE

FINAL YEAR PROJECT PROPOSAL

TOPIC: SMART AND SECURE CLOUD FILE SHARING SYSTEM WITH AI-DRIVEN INSIGHTS.

BY

EUGENE DOKYE ANOKYE, 8534621

JEDIDIAH AMPADU-AMEYAW, 8532821

SUPERVISOR:

DR. BENJAMIN TEI PARTEY

TABLE OF CONTENTS

1. INTRODUCTION/BACKGROUND

With the increasing need for digital collaboration, cloud-based file-sharing systems have become indispensable tools in both personal and professional environments. Services like **Google Drive**, **Dropbox**, and **WeTransfer** offer convenience but often come at the cost of security vulnerabilities, including potential data breaches and unauthorized access.

As data privacy regulations tighten worldwide, secure file sharing has become a critical concern for businesses and individuals alike.To address these challenges, this project proposes the development of a **Smart and Secure Cloud-Based File Sharing System** with **End-to-End Encryption** and **AI-powered security features**. Unlike traditional systems, this system will proactively detect security threats, prevent data leaks, and enhance user experience through intelligent automation.

2. PROBLEM STATEMENT

Current cloud-based file-sharing solutions prioritize ease of use and accessibility but often fall short in providing **robust security** and **intelligent threat detection**. Users risk **unauthorized access**, **data leaks**, and **phishing attacks** without adequate safeguards in place. Furthermore, manually managing access permissions and organizing files can be cumbersome and error-prone, leading to accidental data exposure.

Existing solutions lack:

- **Proactive AI-driven threat detection** to identify suspicious activity.
- **Automated Data Loss Prevention (DLP)** mechanisms to flag sensitive information before sharing.
- **Context-aware access control** to simplify and secure file-sharing processes.
- **Accessibility enhancements** like **voice-activated search** for hands-free, intuitive interactions.

3. PROBLEM SCOPE

This project will focus on designing and developing a secure, cloud-based file-sharing system with the following key features:

a) **End-to-End Encryption (E2EE):**
Ensuring that files are encrypted on the user's device before being uploaded to the cloud and can only be decrypted by authorized recipients.

b) **AI-Powered Threat Detection:**
Implementing machine learning algorithms to monitor file-sharing activities and detect anomalies indicative of unauthorized access or malicious intent.

c) **Data Loss Prevention (DLP):**
Using AI and Natural Language Processing (NLP) to scan files for sensitive data (e.g., personal information, financial details) and alert users before sharing.

d) **Context-Aware Smart Permissions:**
Leveraging AI to suggest optimal access permissions based on user behavior, file content, and sharing history.

e) **Voice-Activated File Management:**
Integrating voice recognition for hands-free file search, navigation, and sharing to improve accessibility

4. PROJECT AIM AND OBJECTIVES

Aim:
To develop a **smart, secure, AI-enhanced cloud-based file-sharing system** that ensures data privacy, detects security threats proactively, and enhances user experience with intelligent automation.

Objectives:

1. Design and implement an **end-to-end encryption** protocol for secure file transfers.
2. Develop **AI models** for real-time **anomaly detection** in file-sharing behavior.
3. Integrate **Data Loss Prevention (DLP)** mechanisms to identify and flag sensitive information before files are shared.
4. Create a **context-aware access control** system using machine learning to recommend permissions.
5. Implement a **voice-activated interface** for intuitive file management.
6. Ensure the system is **scalable** and **user-friendly**, with a modern, responsive UI.

5. JUSTIFICATION

This project addresses the growing need for **secure and intelligent file-sharing solutions** in a world where data breaches and privacy violations are increasingly common. By integrating AI for **proactive threat detection** and **data loss prevention**, this system will offer a **significant improvement over existing services**.

Key differentiators include:

- **AI-Powered Security:** Most existing systems are reactive to threats, while this system will **predict and prevent** them using advanced AI models.
- **Enhanced Data Privacy:** Through **automated DLP**, users will be protected from accidentally sharing sensitive data, a feature largely absent in current solutions.
- **Accessibility:** The **voice-activated interface** will cater to users who prefer hands-free interactions, making the system more inclusive.
- **User-Centric Design:** AI-driven **smart permissions** will streamline the file-sharing process, reducing manual errors and enhancing security.

The project is both **technically challenging** and **highly relevant**, offering an opportunity to work at the intersection of **cloud computing, cybersecurity, and artificial intelligence**.

6. SOFTWARE AND HARDWARE REQUIREMENTS

Software Requirements:

- **Programming Languages:** Python (for backend and AI models), JavaScript (React.js for frontend)
- **Frameworks:** Django (backend), TensorFlow (AI models), React.js (frontend)
- **Security Tools:** OpenSSL (for encryption), OAuth 2.0 (for authentication)
- **Databases:** MySQL (for metadata and user information)
- **APIs & Libraries:** Google Speech-to-Text API (for voice commands), spaCy/NLTK (for NLP tasks)

Hardware Requirements:

- **Development Environment:** Standard laptop/desktop
- **Testing Devices:** Mobile devices (Android/iOS) for testing the responsive UI and voice commands.

7. CONCLUSION

This project aims to revolutionize cloud-based file sharing by combining **end-to-end encryption** with **AI-driven security features**. By addressing current limitations in existing systems—such as lack of proactive threat detection and data loss prevention—this solution will offer users unparalleled security and convenience. Furthermore, the integration of **smart permissions** and **voice-activated features** will provide a more seamless and accessible user experience.

The proposed system not only meets the growing demand for **secure file-sharing** but also pushes the boundaries by incorporating **advanced AI technologies** to **proactively protect** user data.

8. REFERENCES

- Amazon Web Services. (n.d.). *AWS Cloud Security*. Retrieved from https://aws.amazon.com/security/
- Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.
- Microsoft Azure. (n.d.). *Azure Cognitive Services Documentation*. Retrieved from https://azure.microsoft.com/en-us/services/cognitive-services/
- OpenAI. (n.d.). *GPT and AI Models for Natural Language Processing*. Retrieved from https://openai.com/
- OWASP Foundation. (n.d.). *OWASP Top 10 Security Risks*. Retrieved from https://owasp.org/www-project-top-ten/
- Tan, P.-N., Steinbach, M., & Kumar, V. (2019). *Introduction to Data Mining*. Pearson.