AI-Enhanced Dual-Server Encryption for Secure Cloud Search

Abstract

With the rise of cloud computing, ensuring both security and efficient searchability over encrypted data has become a crucial challenge. Traditional Public Key Encryption with Keyword Search (PEKS) systems suffer from inefficiencies and vulnerabilities, such as keyword guessing attacks (KGA) and slow search performance. This project introduces AI-Driven Dual-Server Public Key Encryption with Keyword Search (AI-DS-PEKS) to enhance secure cloud storage. The core enhancement is an AI-driven keyword search optimization, which leverages machine learning (ML) to improve search efficiency and reduce redundancy in keyword searches. Additionally, we integrate post-quantum cryptographic methods to future-proof encryption against quantum threats. The system will be implemented on AWS (Amazon Web Services) cloud, utilizing RSA and other encryption techniques to ensure confidentiality and security.

Objectives

The main objectives of this project are:

- Enhancing Search Efficiency: Implement an AI-based approach to optimize search queries, reducing computation time and improving retrieval speed.
- Ensuring Data Privacy: Prevent unauthorized access by encrypting data before storing it in the cloud.
- Mitigating Keyword Guessing Attacks (KGA): Use AI techniques to detect anomalous search patterns and improve keyword trapdoor security.
- Ensuring Long-Term Security: Adopt post-quantum cryptographic algorithms to resist quantum computing attack

Key Features

1. Dual-Server Model:

Splits encrypted data and search operations across two independent cloud servers to enhance security.

2. AI-Driven Keyword Search Optimization:

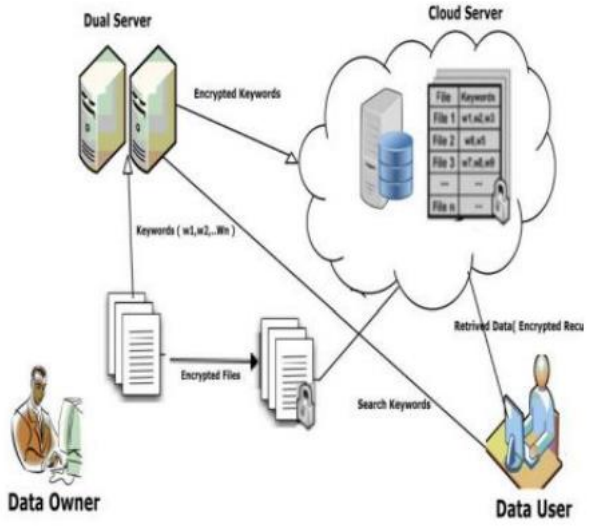
Uses machine learning to predict frequent search terms, optimize trapdoor generation, and reduce search time.

3. Public Key Encryption (RSA & other):

Ensures that only authorized users can decrypt the stored data.

4. Zero-Knowledge Proof Authentication: Allows secure searches without revealing keywords or content to the cloud provider.

ARCHITECTURE DIAGRAM



Proposed System & Enhancements

Our project improves upon existing DS-PEKS systems by introducing:

AI-Driven Keyword Search Optimization

Machine learning algorithms predict and prioritize keyword searches, improving performance.

Reduces redundant queries by learning from previous search patterns.

Post-Quantum Cryptographic Security

Uses other algorithm to resist attacks from future quantum computers.

Working of the System

Encryption & Upload

User encrypts data using RSA/other algorithm before uploading it to AWS cloud storage.

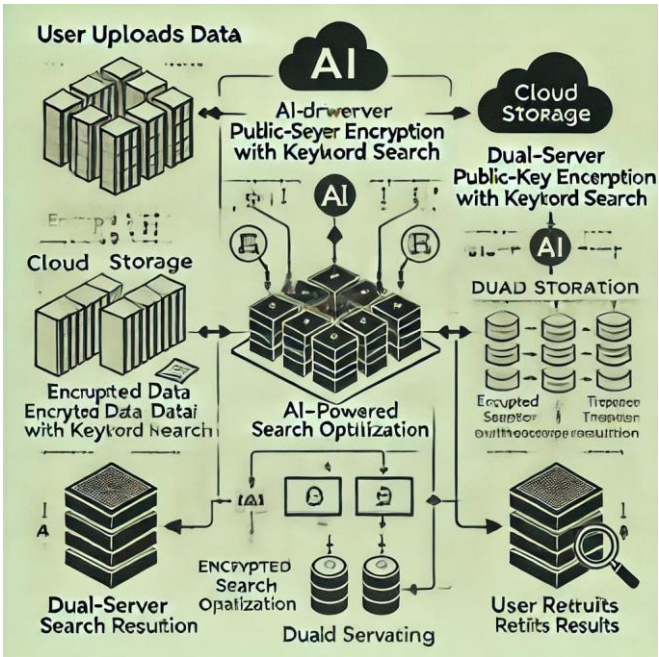
A searchable encrypted index is generated and stored with the data.

AI-Optimized Keyword Search

When a search query is made, AI analyzes search trends and optimizes the query generation.

A trapdoor (encrypted search token) is created and sent to the cloud.

BLOCK DIAGRAM FOR PROPOSED ENHANCEMENT



Dual-Server Processing

Two cloud servers independently process the search request without decrypting the data.

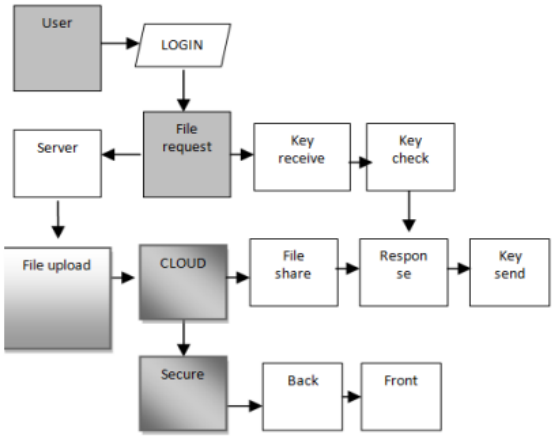
Decryption & Retrieval

The encrypted results are returned to the user, who decrypts them using their private key.

Expected Outcomes

- Faster Keyword Searches: AI optimization significantly reduces search time.
- Quantum-Safe Encryption: other encryption secures data against quantum threats.
- Improved Privacy: Zero-Knowledge Proofs prevent unauthorized access to search terms.

BLOCK DIAGRAM



Applications

- Secure Cloud Storage for Enterprises: Ensures confidential document storage and retrieval.
- Medical & Legal Records Management: Protects sensitive client data while enabling secure searches.
- Government & Defense Data Security: Provides high-level encryption and tamper-proof logging for classified information.

Conclusion:

This research enhances Dual-Server Public Key Encryption with Keyword Search (DS-PEKS) for secure cloud storage. By integrating AI-based search optimization, blockchain security, and post-quantum encryption, we improve efficiency, security, and privacy.

The system allows users to store and search encrypted data without revealing sensitive information to the cloud provider. Future work includes enhancing AI models for better search efficiency and expanding post-quantum cryptography techniques to further strengthen security against emerging threats.