# Privacy-Preserving Data Sharing Platform

## Introduction

In today’s data-centric landscape, the ability to share information securely and efficiently among multiple parties has become an essential requirement across various sectors. However, traditional data-sharing methods are often fraught with risks, leading to breaches of privacy and exposure of sensitive information. This is particularly concerning in domains such as healthcare, finance, research, and legal industries, where data confidentiality is critical, and compliance with stringent privacy regulations is mandatory.  
  
The Privacy-Preserving Data Sharing Platform seeks to address this pressing issue by offering a comprehensive and innovative solution for secure data exchange. The platform leverages cutting-edge technologies, such as advanced encryption methods, fine-grained access control, and privacy-preserving techniques like differential privacy, homomorphic encryption, and secure multiparty computation. These technologies ensure that sensitive data remains protected while still enabling collaborative analysis and decision-making.  
  
This platform is designed to balance the dual objectives of utility and security, allowing stakeholders to harness the full potential of shared data without compromising its integrity, confidentiality, or compliance with ethical standards. By fostering trust and encouraging seamless collaboration, the platform aims to pave the way for a new era of responsible and privacy-conscious data sharing in interconnected ecosystems.

## Problem Statement

Sharing data among multiple parties is vital across industries but poses significant challenges related to privacy and security. Sensitive information, such as personal data, financial records, or proprietary insights, is often vulnerable to breaches, misuse, and regulatory non-compliance. Traditional data-sharing methods either overly restrict access, limiting collaboration, or fail to provide adequate privacy safeguards.  
  
The Privacy-Preserving Data Sharing Platform addresses this issue by enabling secure and efficient data sharing while protecting sensitive information. Using advanced technologies like encryption, secure computation, and access controls, it ensures data confidentiality and compliance with privacy regulations, fostering trust and promoting innovation in data-driven ecosystems.

## Objectives

* To implement secure access through Multi-Factor Authentication (MFA), such as OTP-based verification.
* To securely exchange encryption keys using asymmetric encryption (RSA).
* To encrypt all shared data (text, files) using AES for confidentiality.
* To allow decryption only for authorized recipients with valid RSA private and AES keys.
* To enable secure collaborative computation through privacy-preserving techniques like SMPC.
* To ensure compliance with privacy regulations like GDPR and HIPAA.
* To maintain a tamper-proof record of data sharing activities for transparency.

## Literature Survey

This section reviews existing concepts and techniques related to privacy-preserving data sharing, encryption, secure computation, and access control mechanisms, along with their relevance to privacy compliance and data auditing.

|  |  |  |
| --- | --- | --- |
| Concept | Description | Techniques Used |
| Privacy-Preserving Data Sharing | The process of sharing data among multiple parties while ensuring that sensitive information is protected. | Encryption (AES, RSA), Anonymization (SHA-256), Differential Privacy, Secure Multi-Party Computation. |
| Encryption for Data Security | Ensures that data remains confidential during storage and transmission by making it unreadable to unauthorized users. | AES encryption, RSA for key exchange, TLS for secure communication. |
| Secure Multi-Party Computation | Allows multiple parties to compute a function over their inputs without revealing individual data points. | Homomorphic Encryption, Secret Sharing, Oblivious Transfer. |
| Access Control Mechanisms | Restricts data access to only authorized users to prevent unauthorized data usage or tampering. | RBAC, ABAC, MFA. |
| Compliance with Privacy Laws | Ensures that data-sharing practices adhere to legal and regulatory standards protecting user privacy. | GDPR, HIPAA. |
| Data Provenance and Auditing | Tracks the origin and access history of shared data, ensuring accountability and transparency. | Timestamping, Audit trails, Digital signatures. |
| Data Minimization | Ensures that only the necessary amount of data is collected and shared, reducing risk of overexposure. | Data masking, Tokenization, Data aggregation. |
| Privacy-Preserving Cloud Computing | Enables secure and private data computation in cloud environments while ensuring confidentiality. | Encrypted data processing, Secure enclaves, Trusted Execution Environments. |

## Research Gap

Despite the progress made in privacy-preserving data-sharing techniques, several challenges remain in finding the right balance between data security, efficiency, and regulatory compliance. Most current solutions tend to focus on specific areas independently, rather than combining these techniques into a unified system.  
  
While AES and DCT have shown success in protecting data and improving efficiency, there is limited research on their combined application for large-scale, multimedia data. Furthermore, access control models like RBAC are not well-explored in multi-user data-sharing contexts such as healthcare. There is also insufficient exploration of federated and policy-compliant models that meet GDPR and HIPAA standards while maintaining interoperability.

## Security Concepts Used

Multi-Factor Authentication (MFA) with OTP: OTP generation via TOTP provides a robust second layer of security, protecting against unauthorized access.

RSA for Asymmetric Key Encryption: RSA enables secure key exchange; only the intended recipient can decrypt and retrieve the AES key.

AES for Symmetric Key Encryption: AES encryption provides confidentiality for both text and image data, protecting sensitive content.

Access Control: Restricts access to data based on user roles, ensuring only authorized users can view or modify data.

Secure Multi-Party Computation (SMPC): Allows multiple parties to compute functions on their private inputs without revealing them.

## Innovation

Selective Client Messaging allows the sender to target individual users or groups, ensuring that sensitive information is shared only with relevant parties. This enhances privacy and usability.  
  
Dynamic Key Rotation ensures that each session generates a new AES key distributed securely via RSA encryption. Even if one key is compromised, others remain protected, aligning with cryptographic best practices.

## Methodology

1. Dynamic Receiver Selection  
- Allow sender to select specific recipients through a secure interface.  
- Enable group or individual messaging for controlled communication.  
  
2. Hybrid Encryption Framework for Text Messages  
- Use AES for message encryption and RSA for key distribution.  
- Generate unique session-specific AES keys for each message.  
  
3. Secure Decryption at Receiver Side  
- Recipients decrypt AES key using RSA private key, then decrypt message using AES key and verify via MACs.