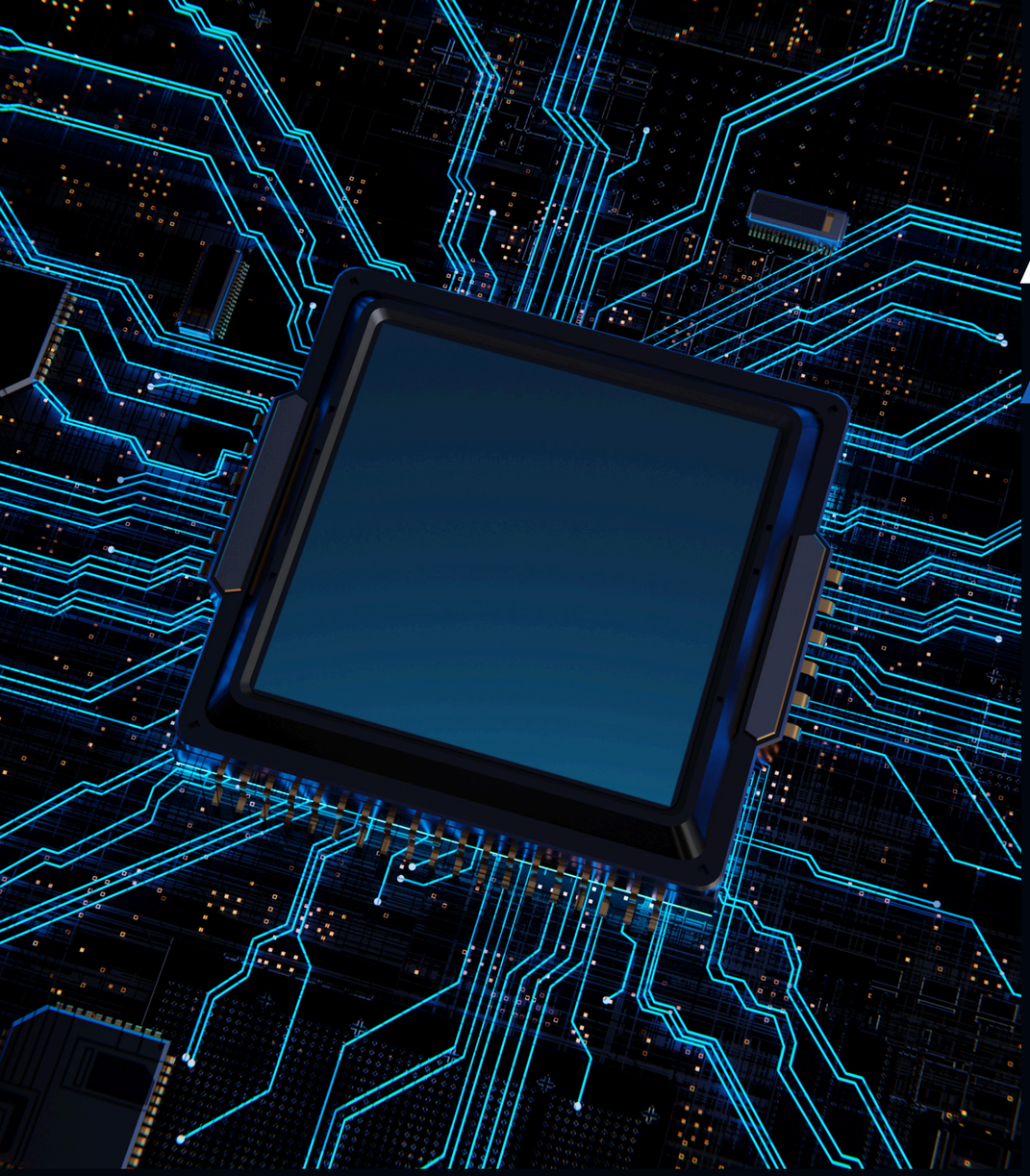
SECURE MESSAGING

Salemdes Application



ABOUT OUR APPLICATION

This project is a Secure Messaging Application designed to protect confidential communication using modern cryptographic techniques. The system simulates a corporate messaging environment where privacy, authenticity, and message integrity are critical. The focus of the project is not only on using cryptography, but on integrating it correctly into a secure system.

OUR AMAZING TEAM

Didar Nurdaulet

Cryptography &
Messaging Lead

Nuradil Kanat

Blockchain &
Integration Lead

Sherkhan Kudaibergen

Authentication &
Security Lead

PROBLEM STATEMENT

Weak protection

Lack of verifiable privacy in mainstream messaging apps.

Encryption

Need for secure, client-side file encryption.

Audit

Absence of transparent audit trails for sensitive operations.

Cyber attack

Protection against cyber attacks with cutting-edge detection.

ARCHITECTURE OVERVIEW

System Design

The application is built on a modular architecture consisting of four core components:

Secure Messaging System

Handles real-time, encrypted communication between users

Blockchain Audit Ledger

A decentralized ledger that records critical system events to preventing tampering.

File Encryption Module

Provides tools for securing sensitive documents locally.

Custom Cryptography Library

A collection of cryptographic primitives implemented from scratch for educational and auditing purposes.

CORE FEATURES

End-to-End Encryption

Forward Secrecy

Authentication

FILE ENCRYPTION MODULE

Functionality: Enables users to encrypt and decrypt files securely before they leave the device or for local storage.

Workflow:

Key Derivation: Information from the user's password is hardened using PBKDF2 to generate a strong encryption key.
Encryption: The file content is encrypted using AES-256-GCM, which provides both confidentiality and integrity checks.
Hashing: A SHA-256 hash is generated to detect any tampering with the encrypted file.
User Benefit: Users can safely store files on cloud services or potential insecure environments, knowing that without the password, the data is inaccessible.

CUSTOM CRYPTOGRAPHY LIBRARY

Implemented Algorithms:

AES

Implementation of the Advanced Encryption Standard key expansion and state transformations.

RSA

Identify and analyze the origins of security threats to improve defenses and prevention strategies.

SHA-256

Simplified implementation of the secure hash standard.

Classic

Caesar Cipher (with frequency analysis breaker), Vigenère Cipher (with Kasiski examination).

Educational Value: A unique feature of Salemdes is its "from scratch" implementation of classic and modern algorithms. This serves to demonstrate a deep understanding of cryptographic principles.

SECURITY ANALYSIS

THREAT MODEL

Designed to withstand compromised servers and network interception (Man-in-the-Middle attacks).

ZERO-KNOWLEDGE ARCHITECTURE

The server does not know the users' private keys or passwords

INTEGRITY CHECKS

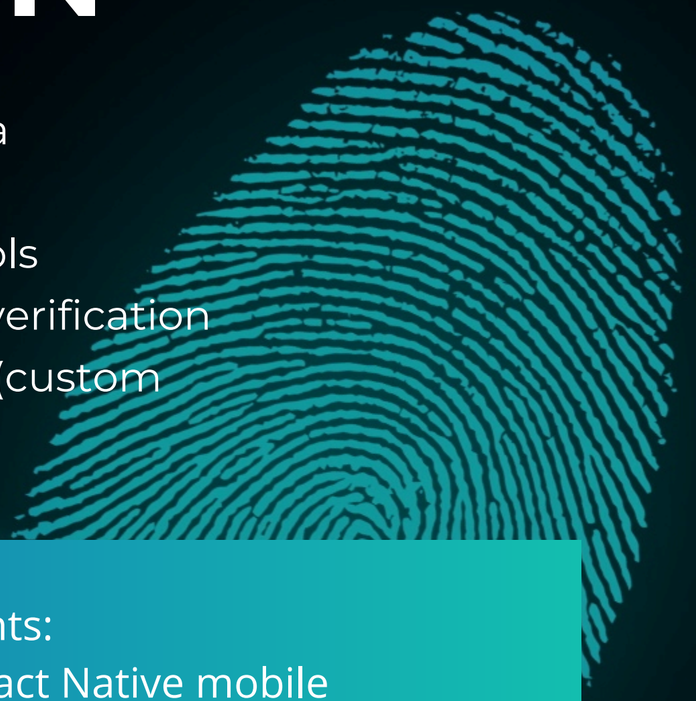
All data (messages, files, blockchain blocks) is cryptographically signed or hashed.

ATTACK MITIGATION

Brute Force, Replay Attacks,Tampering

CONCLUSION

Salemdes successfully demonstrates a comprehensive approach to modern cybersecurity, combining practical tools (messaging, file sync) with advanced verification (blockchain) and foundational theory (custom crypto).



Future Improvements:

Mobile App: Development of a React Native mobile application.

Group Chat: Implementing Signal Protocol for multi-party encryption.

P2P Transfer: Direct peer-to-peer file sharing via WebRTC.