ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 12, Issue 1, January 2025

VaultBox: A Comprehensive Secure Communication and Data Management Platform

S. S. Jogdand , Manthan Marathe, Ameya Kawade, Rushikesh Maddewad, Sanskar Ubale

Professor, Department of Computer Engineering, PC Polytechnic, Pimpri Chinchwad, Maharashtra, India
Student, Department of Computer Engineering, PC Polytechnic, Pimpri Chinchwad, Maharashtra, India
Student, Department of Computer Engineering, PC Polytechnic, Pimpri Chinchwad, Maharashtra, India
Student, Department of Computer Engineering, PC Polytechnic, Pimpri Chinchwad, Maharashtra, India
Student, Department of Computer Engineering, PC Polytechnic, Pimpri Chinchwad, Maharashtra, India

ABSTRACT: The proliferation of digital communication and data sharing has exposed critical vulnerabilities in existing secure communication platforms. VaultBox emerges as an innovative solution, integrating advanced security technologies to address comprehensive data protection challenges. By leveraging lattice-based Kyber encryption, publish-subscribe (Pub/Sub) architecture, VaultBox provides a robust, end-to-end secure platform for sensitive data management and communication.

KEY WORDS: Data Security, Kyber Encryption, Publish-Subscribe Architecture, Secure Communication, Role-based Access Control

I. INTRODUCTION

The rapid digitalization of personal and professional activities has resulted in an unprecedented volume of sensitive data generation. Existing storage solutions, such as traditional cloud platforms, often fail to strike a balance between robust security and ease of use, exposing users to potential cyber threats. Additionally, features like encrypted sharing, role-based access control, real-time synchronization, and privacy-preserving communication remain inadequately addressed.

A. *Types of Data Management Challenges*

- Insufficient encryption measures.
- Vulnerability to unauthorized access.
- Lack of advanced sharing capabilities.
- Insecure or third-party-dependent video conferencing solutions.

B. *Motivation:*

- Rising cases of data breaches and phishing attacks.
- Increasing need for compliance with global data privacy regulations.
- Demand for secure, scalable storage and private communication solutions.

C. Solution:

- Lattice-based Kyber encryption
- Publish-subscribe communication architecture
- Role-based access contro
- Self-hosted communication infrastructure

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 12, Issue 1, January 2025

II. SIGNIFICANCE OF THE SYSTEM

VaultBox aims to revolutionize secure data management and communication by addressing gaps in traditional systems. Its key features include lattice-based Kyber encryption, client-side key management, role-based access control (RBAC), real-time synchronization, and privacy-first video conferencing using custom-hosted Jitsi Meet. VaultBox's unique value proposition lies in its ability to combine cutting-edge security protocols with exceptional user experience, catering specifically to organizations prioritizing data privacy.

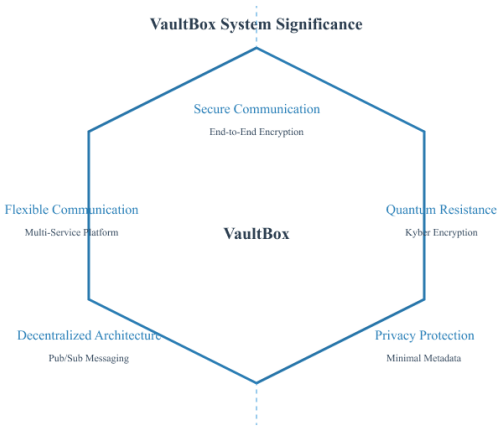

Figure 1: System Significance

III. LITERATURE SURVEY

The literature reveals significant shortcomings in current solutions, which VaultBox seeks to address. Existing systems often prioritize specific functionalities at the expense of holistic security, scalability, or usability, leaving critical gaps for sensitive data management and communication.

A. Traditional Storage Platforms

Existing digital storage solutions demonstrate significant limitations:

- Centralized architectures vulnerable to single points of failure
- Minimal user-controlled encryption mechanisms
- Inadequate secure collaboration features
- Limited cross-platform compatibility

B. Encrypted Messaging Platform

Contemporary encrypted messaging platforms exhibit critical constraints:

- Primarily focused on individual communication
- Server-side encryption vulnerabilities
- Limited file storage capabilities
- Restricted synchronization across devices

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 12, Issue 1, January 2025

C. Enterprise File Management Systems

Existing enterprise solutions present notable challenges:

- Complex implementation requirements
- Prohibitive cost structures
- Legacy encryption methodologies
- Limited flexibility in hosting infrastructure

D. Emerging Cryptographic Technologies

Recent advancements highlight crucial research directions:

- Lattice-based encryption's quantum resistance
- Distributed communication architectures
- Enhanced privacy-preserving technologies

IV. METHODOLOGY

The VaultBox architecture comprises five interconnected modules designed to provide a secure, efficient, and privacy-focused platform for data management and communication.

A. System Architecture

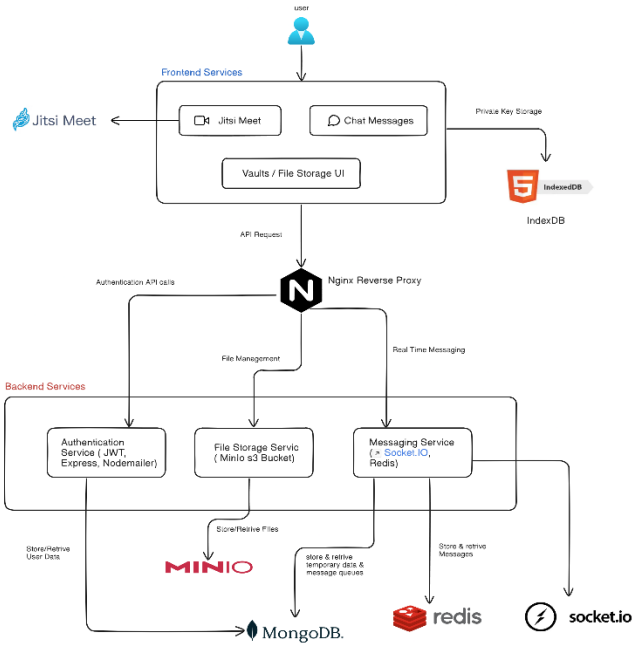

Figure 2: Architecture Diagram

1. Authentication Module

- Implements custom OTP-based authentication using a self-hosted Nodemailer service.

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 12, Issue 1, January 2025

- Ensures client-side key management to protect user credentials and session data.
- Utilizes JWT tokens for secure session handling.

2. **Data Storage Module**
   - Employs AES-256 encryption for data security and lattice-based Kyber encryption for message and file exchanges**.**
   - Splits files into encrypted chunks stored with metadata in MongoDB.
   - Ensures keys are securely managed on the client side to prevent unauthorized server access.

3. **Sharing Module**
   - Allows secure sharing through time-limited, password-protected links.
   - Integrates RBAC to restrict access and provide granular control over permissions.
   - Leverages JWT tokens for efficient and secure role enforcement.

4. **Communication Module**
   - Integrates custom-hosted Jitsi Meet for private, secure video conferencing.
   - Ensures all meetings are hosted on independent servers for privacy-sensitive organizations.
   - Encrypts communication using end-to-end protocols and lattice-based security enhancements.

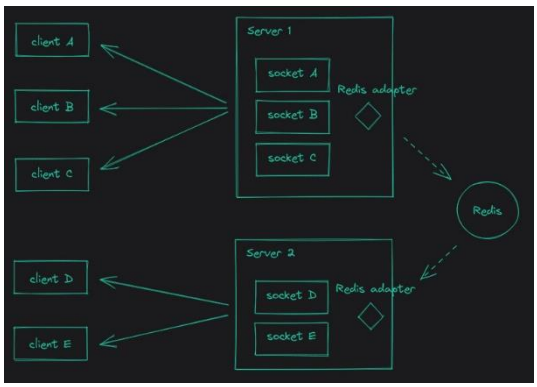

Figure 3: Publish Subscribe Architecture

V. CONCLUSION AND FUTURE WORK

VaultBox represents a significant advancement in secure data management and communication. Its innovative architecture combines lattice-based encryption, client-side key management, RBAC, and custom-hosted video conferencing to address the limitations of traditional platforms. Future work will focus on:

- Integrating blockchain for tamper-proof audit logs.
- Leveraging AI for predictive analytics and enhanced data organization.
- Expanding offline functionality and scalability for large enterprises.

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 12, Issue 1, January 2025

VI . ACKNOWLEDGEMENT

We extend our heartfelt gratitude to our project guide, Prof. S.S. Jogdand, for his invaluable support and guidance throughout this project.

REFERENCES

1. Zhang, L., et al. (2022). "Predictive Analytics in Data Management." Data Science Journal, 12(3), 78-92.
2. Brown, M. (2023). "Modern File Management Systems: A Comprehensive Review." Tech Innovation Quarterly, 9(1), 15-30.
3. Albrecht, M., et al. (2023). "Kyber: Quantum-Resistant Encryption Algorithms." Cryptography Advances Journal, 15(2), 200-220.