st

Rotarix

Hack Vortex 2025

Viva Institute of Technology Mumbai

Rotarix: AI-Powered, Quantum-Resistant Key Rotation for Next-Gen Security

TEAM NAME : JNR

INSITUTION : Shiv Nadar University, Chennai

TRACK THEME : Cybersecurity

TEAM MEMBERS : Jayashre (TL), Nidhi Gummaraju, Roahith R

Lovable

LifeLine

Rotarix

ABOUT TEAM

JNR

Jayashre K

Nidhi Gummaraju

Roahith R

Lovable

LifeLine

PROBLEM STATEMENT

In 2017, Equifax, one of the largest credit reporting agencies, experienced a catastrophic data breach exposing sensitive information of approximately 147 million individuals. A significant factor contributing to this breach was poor key rotation practices and the use of weak encryption protocols, which allowed attackers to bypass encryption and access unprotected data.

Current Key Rotation Challenges:

Predictable & Manual – Static schedules make rotations easy targets for attackers.

Compliance Hassles – Meeting PCI-DSS, GDPR, HIPAA is tough with outdated methods.

Quantum Threats – Future quantum attacks could break existing encryption.

Need for Smarter Solution:

AI-Driven Rotation – Adaptive, risk-based key updates for real-time security.

Quantum-Resistant Crypto – Future-proof encryption against emerging threats.

Zero-Trust & Auditability – Immutable logs & no blind trust in any entity.

ABSTRACT

Rotarix is an **AI-powered, quantum-resistant key rotation system** that enhances security by dynamically adjusting key lifetimes based on risk levels. Unlike traditional fixed-interval rotations, **Rotarix** uses machine learning to predict threats, ensuring proactive key updates. It integrates **blockchain-backed auditability**, **multi-cloud compatibility**, and **post-quantum cryptography** to deliver a future-proof, zero-trust security model.

Key Innovations

- **AI-driven key rotation** based on anomaly detection
- Quantum-resistant cryptographic algorithms (e.g., CRYSTALS-Kyber)
- Blockchain-backed immutable audit logs
- Zero-trust access control
- Self-healing keys & dynamic MFA adapt instantly to threats.

HOW IT DIFFERS FROM THE EXISTING SYSTEM

Feature	Traditional Key Rotation	Rotarix (Our Proposed Solution)
Rotation Method	Fixed Time-Based	AI-Driven, Adaptive
Threat Response	Delayed	Real-Time Detection & Response
Quantum Resistance	No	Yes (Post-Quantum Cryptography)
Auditability	Centralized Logs	Blockchain-Based Immutable Logs
Security Model	Static	Zero-Trust & Dynamic

COMPONENTS USED / SOFTWARE TOOLS

Rotarix

AI/ML

(for anomaly detection)

TensorFlow

PyTorch

Blockchain

(immutable key logs)

Hyperledger FABRIC

ethereum

Security Framework

ZERO TRUST

NIST National Institute of Standards and Technology

Cryptography

(quantum-resistant keys)

CRYSTALS

AES-256 ENCRYPTION

RSA

Key Management

HashiCorp Vault

OpenSSL Cryptography and SSL/TLS Toolkit

Database

(for secure key storage)

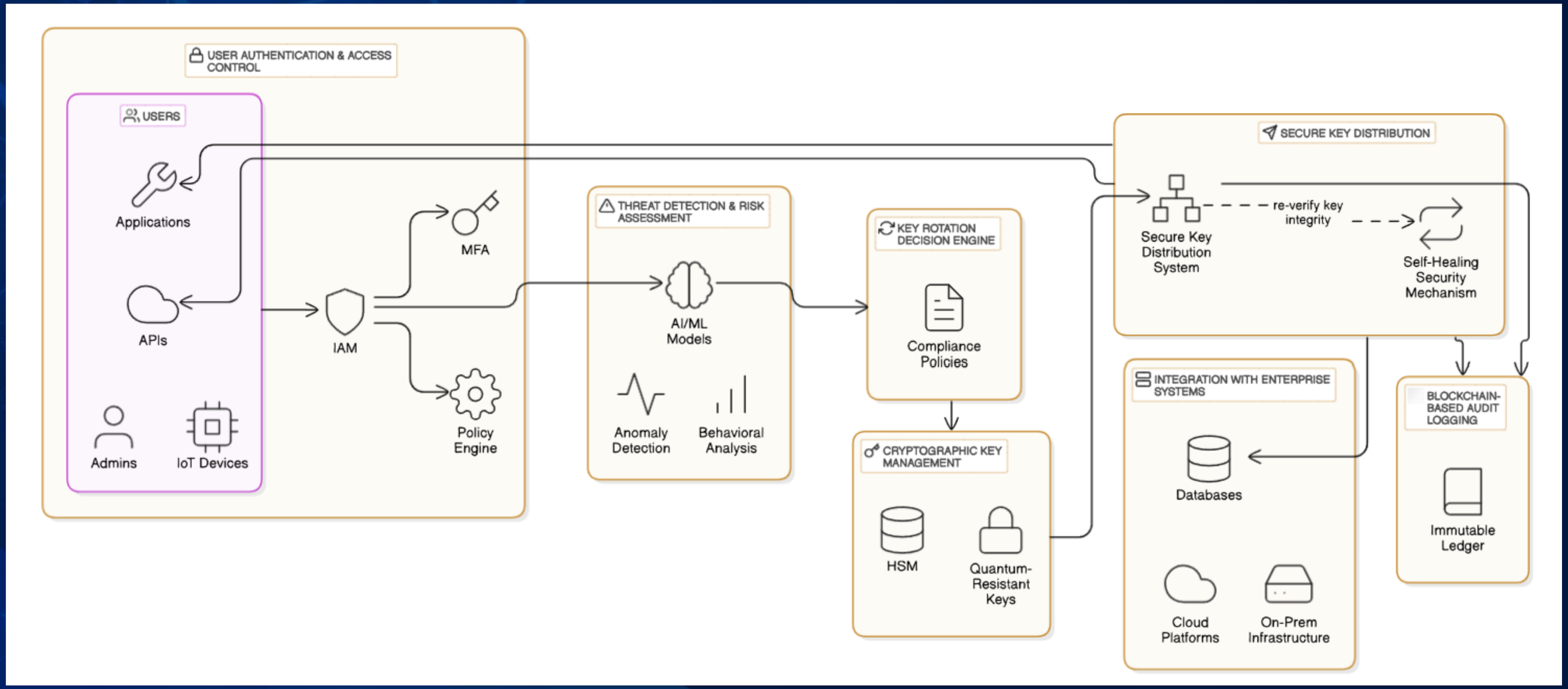
PostgreSQL

SQLite

Lovable

LifeLine

ARCHITECTURE DIAGRAM



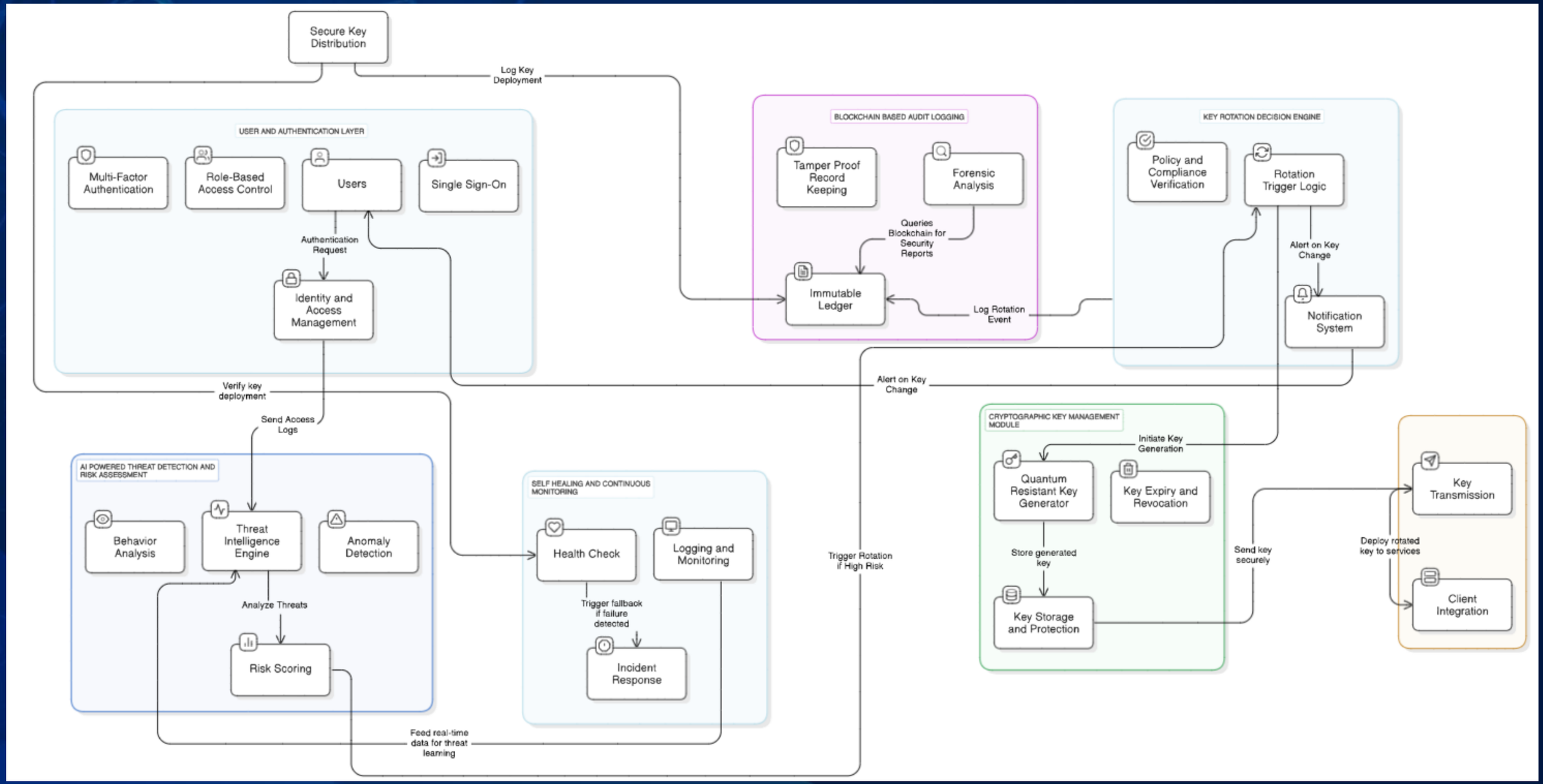
Rotarix

Lovable

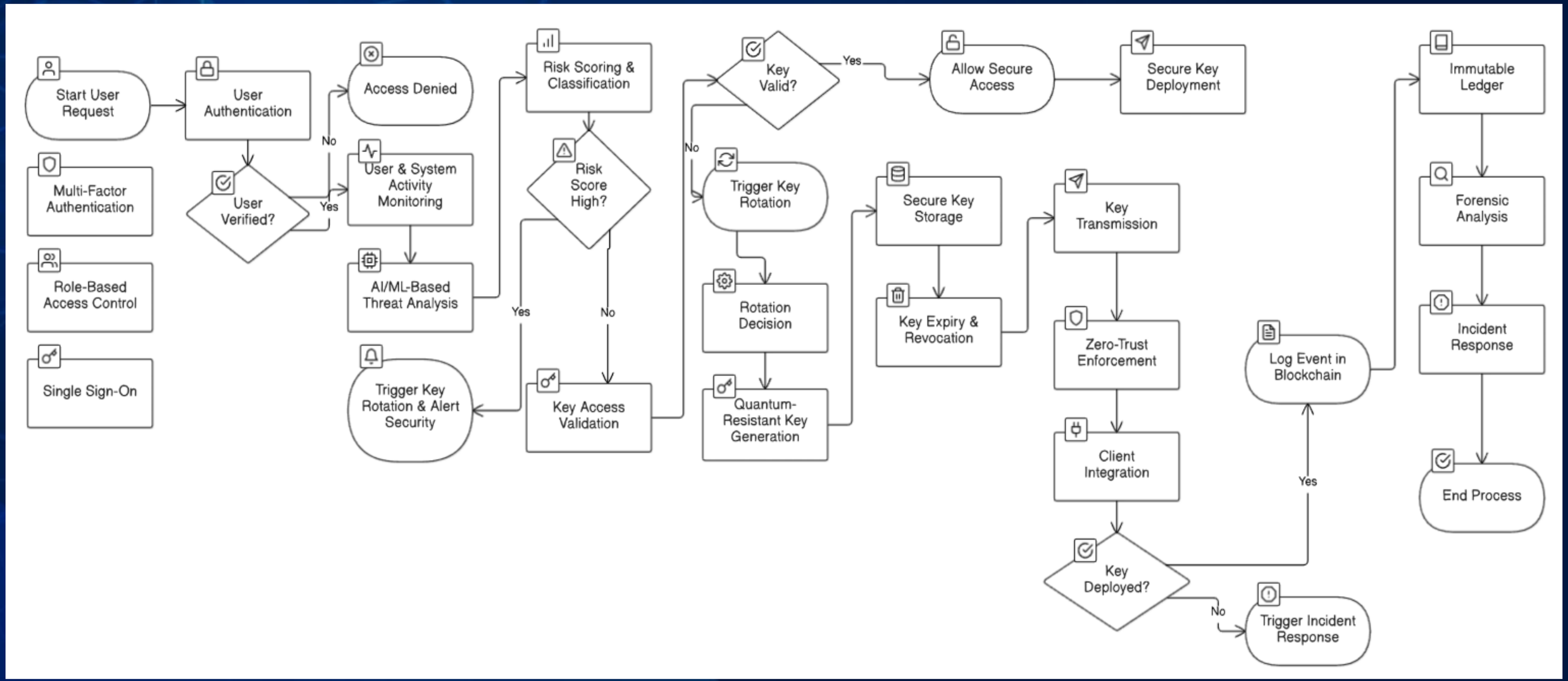
LifeLine

BLOCK DIAGRAM

Rotarix



FLOW CHART


Start User Request
Multi-Factor Authentication
Role-Based Access Control
Single Sign-On
User Authentication
User Verified?
No
Yes
Access Denied
User & System Activity Monitoring
AI/ML-Based Threat Analysis
Trigger Key Rotation & Alert Security
Risk Scoring & Classification
Risk Score High?
Yes
No
Key Access Validation
Key Valid?
No
Yes
Trigger Key Rotation
Rotation Decision
Quantum-Resistant Key Generation
Allow Secure Access
Secure Key Deployment
Secure Key Storage
Key Expiry & Revocation
Key Transmission
Zero-Trust Enforcement
Client Integration
Key Deployed?
No
Yes
Trigger Incident Response
Log Event in Blockchain
Immutable Ledger
Forensic Analysis
Incident Response
End Process

METHODOLOGY

Rotarix

1. **Risk-Based Key Rotation:** AI-driven models analyze real-time threat levels to trigger key rotation dynamically.
2. **Quantum-Resistant Encryption:** Integrates CRYSTALS-Kyber and AES-256 to future-proof against quantum attacks.
3. **Immutable Key Logs:** Blockchain ensures tamper-proof logging of key rotations for transparency and auditability.
4. **Zero-Trust Authorization:** Access control enforced with multi-factor authentication and contextual verification.
5. **Automated Anomaly Detection:** Machine learning detects suspicious activity and initiates proactive security measures.
6. **Efficient Key Lifecycle Management:** Secure generation, storage, rotation, and revocation of cryptographic keys.

Lovable

LifeLine

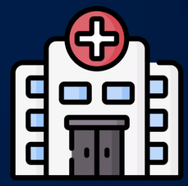
IMPLEMENTATION

Rotarix

Real-World Implementation

Enterprise & Finance:
Automates key management for compliance and secure transactions.

Government & Defense:
Protects sensitive data from cyber and quantum threats.



Healthcare:
Secures patient records and integrates with DevOps pipelines.

Future Impact

Quantum-Resistant Security:
Adapts encryption for evolving threats.

Decentralized Key Management:
Eliminates single points of failure.

Self-Healing Security:
Detects and mitigates key compromise in real-time.

AI-Driven Automation:
Predicts risks and rotates keys autonomously.

IoT & Smart Devices:
Scales for lightweight, secure key rotation.

Global Standards & Compliance:
Shapes future cryptographic security frameworks.

Lovable

LifeLine

PROS AND CONS

PROS

- ✓ AI-driven, adaptive security against evolving threats
- ✓ Prepares for quantum computing risks
- ✓ Blockchain-backed audit trail ensures transparency
- ✓ Seamless integration with cloud security tools
- ✓ Complies with security standards (GDPR, HIPAA, PCI-DSS)

CONS

- × Higher computational cost due to AI and quantum-resistant encryption
- × Requires integration with existing enterprise security systems
- × Blockchain storage costs for audit logs

Rotarix

IEEE | St. Joseph's College of Engineering Student Branch Chapter

LifeLine

CONCLUSION

🔑 **Rotarix** transforms key management with **AI, quantum-resistant security, and blockchain-based auditability**. By proactively rotating cryptographic keys based on risk, it **eliminates predictability**, **enhances compliance**, and **future-proofs security infrastructure**.

Future Score

- Expanding AI models for real-time attack prevention
- Enhancing post-quantum security with newer encryption techniques
- Scaling for IoT & edge computing security

THANK YOU!!

Rotarix

Lovable

LifeLine