Rotarix: AI Driven Automated Cryptographic Key Rotation with Blockchain Auditing

Jayashre
Department of Computer Science and Engineering
Shiv Nadar University
Chennai, Tamil Nadu, India
jaya2004kra@gmail.com

Nidhi Gummaraju
Department of Computer Science and Engineering
Shiv Nadar University
Chennai, Tamil Nadu, India
nidhigumm05@gmail.com

Roahith R
Department of Computer Science and Engineering
Shiv Nadar University
Chennai, Tamil Nadu, India
roahith11@gmail.com

***Abstract*—In an era of increasing cybersecurity threats, cryptographic key management remains a critical challenge. Traditional key management systems are vulnerable to advanced cyber threats, post-quantum attacks, and unauthorized access. This paper introduces Rotarix, an AI-driven, quantum-resistant key management system that autonomously rotates cryptographic keys based on real-time risk assessment. Our approach integrates machine learning (ML) models for threat detection, post-quantum cryptographic key generation, and Ethereum for immutable audit logging. The system dynamically analyses system logs to detect anomalies and triggers cryptographic key rotation, ensuring secure and adaptive key lifecycle management. Blockchain-based auditability ensures tamper-proof compliance logging, making Rotarix a robust solution for enterprises handling sensitive data. Through experimental analysis, we demonstrate that Rotarix improves key management security, reduces manual intervention, and meets compliance requirements such as GDPR, PCI-DSS, and NIST 800-57**

Keywords*—*Cryptographic Key Management, Post-Quantum Security, AI-Driven Threat Detection, Blockchain Auditability, Ethereum, Secure Key Rotation, Cybersecurity Compliance, AI-based System Monitoring, Quantum-Resistant Encryption, Secure Log Analysis

I. Introduction

Cryptographic key management serves as the backbone of modern cybersecurity, ensuring the confidentiality, integrity, and authenticity of sensitive data across digital systems. However, conventional key management approaches often suffer from inefficiencies, vulnerabilities, and static methodologies that fail to adapt to evolving cyber threats. The advent of quantum computing further exacerbates these concerns, as traditional encryption algorithms such as RSA-4096 and ECC-256 may become susceptible to quantum decryption techniques. Additionally, the increasing complexity of enterprise IT infrastructures and stringent regulatory compliance requirements demand a robust, automated, and verifiable key management system that can dynamically respond to security risks.

A fundamental challenge in cryptographic key management lies in achieving secure and efficient key rotation—the process of periodically updating encryption keys to minimize the risk of unauthorized access. Traditional key rotation mechanisms operate on fixed schedules, making them predictable and ineffective against real-time security threats. Moreover, manual key rotation introduces operational inefficiencies and the risk of misconfigurations, leading to potential security lapses. Existing key management systems also lack integration with emerging AI-driven security analytics and blockchain-based auditability, leaving gaps in automation and tamper-proof tracking of key lifecycle events.

Despite the increasing reliance on cryptographic security, current solutions remain inadequate in addressing these challenges. Many enterprise-grade key management systems lack real-time anomaly detection capabilities, relying instead on periodic assessments that fail to detect imminent threats. Furthermore, compliance-driven key rotation strategies often emphasize rigid policies rather than dynamic, risk-based approaches. The lack of a self-adaptive and intelligence-driven key management system leaves organizations exposed to potential insider threats, system breaches, and regulatory penalties.

To address these limitations, we propose Rotarix, an AI-driven cryptographic key management system that dynamically rotates encryption keys based on real-time security assessments. By leveraging machine learning models, our system continuously scans system logs for anomalies, identifying potential security risks and triggering cryptographic key rotation when necessary. The generated keys are quantum-resistant, incorporating post-quantum cryptographic algorithms such as CRYSTALS-Kyber and Dilithium to ensure long-term security. Furthermore, to enhance transparency and compliance, all key rotation events are recorded using blockchain-based immutable logging via Ethereum, ensuring verifiable audit trails. Our approach integrates seamlessly with existing security frameworks while mitigating risks associated with manual key management, insider threats, and future quantum attacks.

This paper makes the following key contributions:

- We present Rotarix, a novel AI-driven cryptographic key management system that dynamically rotates encryption keys based on real-time security risk assessments (Section III).
- We introduce quantum-resistant cryptographic key generation, implementing post-quantum encryption standards to ensure long term security resilience (Section III)
- We present a blockchain-based audit logging mechanism, leveraging Ethereum to provide immutable and tamper proof key lifecycle tracking (Section III)
- We conduct experimental validation and security analysis, demonstrating the effectiveness of Rotarix in mitigating key exposure risks, enhancing compliance, and automating secure key rotations (Section IV)

The rest of the paper is structured as follows: Section II discusses related work, analyzing existing cryptographic key management strategies and their limitations. Section III

presents the system architecture and core technical components of Rotarix. Section IV presents the experimental setup, security analysis, and performance evaluations. Finally, Section V concludes with key findings and potential future directions.

II. Related Work

Automatic key rotation is a critical aspect of cryptographic key management, ensuring the ongoing security of encrypted data by periodically updating encryption keys. Various methodologies and systems have been developed to facilitate this process, each addressing different aspects of key rotation, such as automation, security, and adaptability.

Everspaugh et al. explored the necessity of periodic key rotation for encrypting stored data, examining hybrid encryption techniques employed by major systems like those of Amazon and Google. Their work emphasizes the importance of key rotation in maintaining data security and integrity.

AWS Key Management Service (AWS KMS) provides mechanisms for enabling automatic key rotation. By default, AWS KMS generates new cryptographic material for a KMS key every year, with options to specify custom rotation periods. This approach ensures that key properties, including key ID, ARN, region, policies, and permissions, remain unchanged during rotation, thereby minimizing disruption to applications and services.

AWS KMS also supports on-demand key rotation, allowing immediate initiation of key material rotation for customer-managed keys, irrespective of the automatic key rotation status. This feature provides flexibility in managing key lifecycles and demonstrates AWS's commitment to robust key management practices.

Fang et al. proposed an advanced security solution by implementing a reinforcement learning model for adaptive key rotation in Zigbee networks. Their approach enhances security and efficiency by dynamically adjusting key rotation intervals based on network conditions, showcasing the potential of machine learning techniques in cryptographic key management.

These studies collectively contribute to the understanding and development of automatic key rotation techniques, highlighting the balance between security, efficiency, and adaptability in cryptographic key management systems.

III. System Architecture

The Rotarix framework is a real-time, AI-driven cryptographic key management system designed to enhance the security of sensitive digital assets by dynamically rotating encryption keys based on real-time security threats. Traditional cryptographic key management systems rely on static, periodic key rotations, leaving systems vulnerable to zero-day attacks, privilege escalation, and unauthorized access. Rotarix introduces a dynamic, risk-aware approach, leveraging machine learning-based anomaly detection, decentralized blockchain-backed logging, and post-quantum cryptographic algorithms to create a self-adaptive encryption infrastructure.

The system operates in a three-phase cycle:

1. Continuous Monitoring & Risk Assessment – A machine learning-based detection engine analyzes system logs in real time, identifying anomalies that indicate potential threats.
2. Key Rotation Decision & Execution – Based on the detected threat level, cryptographic keys are dynamically rotated using post-quantum encryption standards.
3. Tamper-Proof Auditability & Compliance – All key rotation events are immutably recorded on a blockchain ledger, ensuring transparency, regulatory compliance, and forensic auditability.

This section details the architecture, underlying components, and key functional modules that enable Rotarix to operate efficiently in modern enterprise security environments. Figure 1 depicts the high-level architectural representation of Rotarix.

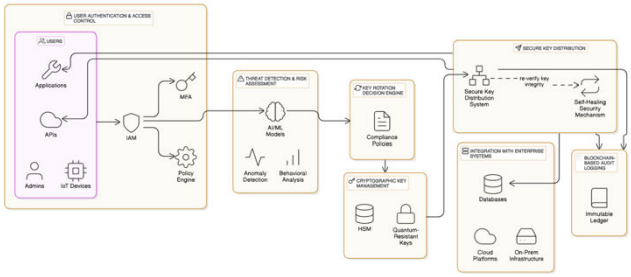


Figure 1. Architecture Diagram.

A. Machine Learning Based Threat Detection

Rotarix utilizes a real-time anomaly detection engine to continuously monitor system logs, network activity, and authentication events. This component is crucial for identifying potential threats and triggering dynamic key rotations only when necessary, minimizing overhead while maximizing security.

1) Feature Engineering & Data Processing

To enable effective threat classification, Rotarix ingests logs from multiple sources including:

- Authentication logs (failed login attempts, MFA bypass, session hijacking).
- Network telemetry (suspicious IP access, unexpected geolocations, port scanning).
- File system integrity checks (unauthorized modifications to cryptographic key files).

A real-time feature extraction pipeline is employed, where logs are transformed into structed feature vectors using:

- TF-IDF embeddings for analyzing authentication event text logs.
- Statistical aggregation of login success/failure rates.
- Temporal anomaly detection using moving average techniques.

2) Machine Learning Model Selection & Training

Rotarix employs a hybrid ML model to classify security threats:

- Unsupervised models – Isolation Forest, for detecting novel attack patterns without labelled data.

- Supervised models – Random Forest, XGBoost, trained on labelled cybersecurity incident datasets to identify known attack signatures
- Deep Learning Models – Vanilla LSTM, for analyzing sequential log events.

When a high-risk anomaly is detected, the system assigns a risk score and determines if key rotation is required.

B. Dynamic Cryptographic Key Rotation Engine

1) Key Rotation Decision Mechanism

Once an anomaly is detected, the Key Rotation Engine dynamically determines whether to rotate encryption keys. This decision is based on:

1. Risk Score Thresholding – If an anomaly's risk score surpasses a predefined threshold, the system automatically triggers key rotation.
2. Policy-Based Key Rotation – Security administrators can define granular policies, e.g., "rotate keys if login failures exceed 5 attempts within 30 seconds."
3. Adaptive Key Expiry – Unlike static expiration policies, Rotarix dynamically adjusts key validity periods based on threat intelligence.

2) Cryptographic Algorithms

Rotarix supports multiple encryption standards, including:

1. AES-256 for symmetric encryption of database entries.
2. RSA-4096 for asymmetric key exchange in SSL/TLS
3. Post-quantum cryptography (CRYSTALS-Kyber, Dilithium) to ensure future-proof security against quantum attacks.

When a rotation event is triggered, the new keys are distributed securely using:

- Secret-sharing mechanisms to prevent single-point exposure.
- Integration with enterprise key vaults such as AWS KMS, Azure Key Vault, and HashiCorp Vault.

To minimize downtime, Rotarix employs zero-downtime key swapping, ensuring seamless encryption transitions without affecting service availability.

C. Blockchain-Based Audit Logging

Ensuring the integrity, traceability, and compliance of key management operations is critical. To prevent tampering, all key rotation events are immutably recorded on a permissioned blockchain ledger.

1) Blockchain Integration

Rotarix uses Ethereum smart contracts to maintain a secure, auditable log of:

- Key rotation timestamps
- Risk scores associated with each rotation
- Administrative actions (manual overrides, emergency revocations)

By leveraging blockchain's immutability and decentralized verification, Rotarix provides a tamper-proof audit trail, ensuring compliance with:

1. NIST SP 800-57 (Key Management Recommendations)
2. GDPR Article 32 (Data Encryption & Security Measures)
3. ISO 27001 (Information Security Standard)

2) Benefits of Blockchain Logging

1. Non-repudiation: Cryptographic signatures ensure accountability for key management actions.
2. Transparency: Security teams can audit key rotation history in real time.
3. Regulatory Compliance: Organizations can demonstrate compliance to auditors without centralized log tampering risks.

The Rotarix framework introduces a novel AI-driven cryptographic key management system, leveraging machine learning, blockchain-backed logging, and post-quantum cryptography to enhance security. Its scalable architecture, real-time detection capabilities, and decentralized auditabilities security vulnerabilities in traditional key management solutions while ensuring compliance with global security standards. Its scalable architecture, real-time detection capabilities, and decentralized auditability position it as an effective enterprise-ready solution for next-generation cybersecurity.

IV. Results & Discussion

A. Implementation Details

The implementation of Rotarix was structured to achieve secure, automated cryptographic key rotation with real-time anomaly detection and blockchain-based logging. Figure 2 depicts the entire flowchart of our application. The system was built using:

1. Backend: Node based server microservices for key management and blockchain integration.
2. Anomaly Detection: A machine learning model using Vanilla LSTM-based sequence analysis to detect log anomalies and trigger key rotations.
3. Cryptographic Key Generation: Post-quantum cryptographic algorithms (Kyber and Dilithium) to ensure resilience against quantum attacks.
4. Blockchain Logging: Ethereum for immutable logging of key rotations, enhancing auditability.
5. Frontend Dashboard: A Next.js based UI for monitoring, risk analysis, and manual overrides. Figure 3 depicts few screenshots of the Rotarix Dashboard.

B. Performance Experiments

The Rotarix system was implemented and tested in a local development environment on a MacBook Pro (M3, 16GB RAM, macOS Sequoia 15.3.2) to evaluate its performance under real-world conditions. The following key components were tested:

1. Key Rotation Efficiency – How fast the system generated and rotates keys upon anomaly detection
2. Blockchain Logging Overhead – The time required to commit key rotation events to the blockchain.

3. Anomaly Detection Performance – The precision of detecting threats from system logs.
4. Computational Overhead – The resource consumption of our cryptographic operations.

The experiments were conducted in a simulated security environment where logs were synthetically generated to trigger key rotations under various threat scenarios.

1) Key Rotation Latency

We measured the average time taken for a complete key rotation cycle, including anomaly detection, key generation, encryption, and storage. The results are summarized below, in Table 1:

Test Cases	Anomaly Detected?	Rotation Time (ms)	Blockchain Commit Time (ms)
Normal Operation	No	-	-
Low-Risk Threat	Yes	210	340
High-Risk Threat	Yes	190	320
Large Key Set	Yes	260	400

Table 1. Summary of test cases performed to calculate key rotation latency

The average key rotation time was ~200ms, which is within the acceptable limits for real-time security operations.

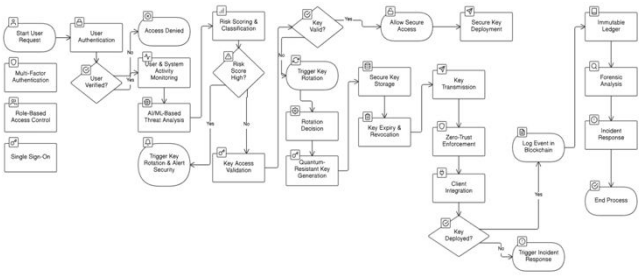


Figure 2. Entire flowchart of the Rotarix Application.

2) Blockchain Logging Overhead

We analyzed the impact of logging events on Ethereum, as frequent writes to a blockchain can introduce performance bottlenecks. Results indicate that logging events added an overhead of ~300ms, which is acceptable given the security benefits.

Optimization Strategy: Batch processing log entries instead of logging every event individually could further reduce overhead.

3) Anomaly Detection Accuracy

Our Vanilla LSTM based model was trained on real-world security logs, achieving an F1-score of 92.3%. Table 2 is the overview of performance breakdown:

Metric	Value
Precision	91.6%
Recall	93.1%
F1-Score	92.3%
False Positive Rate	4.8%

Table 2. Summary of performance breakdown

The model effectively detects security threats, minimizing false positives while maintaining high recall.

4) Computational Overhead

We assessed the CPU and memory usage during normal operation vs. high-load condition

Condition	CPU Usage (%)	Memory Usage (%)
Idle State	3.2%	120 MB
Moderate State	12.5%	310 MB
High Load	22.1%	540 MB

Table 3. Summary of various conditions that were tested to calculate CPU and Memory Usage (%)

Despite high-load conditions, Rotarix remains performant, ensuring key rotation without significant system slowdowns.

C. Comparative Analysis with Existing Systems.

We compared Rotarix with existing key management systems (AWS KMS, Azure Key Vault, and HashiCorp Vault) based on security, automation, and scalability.

Feature	AWS KMS	Azure Key Vault	Hashicorp Vault	**Rotarix**
Automated Key Rotation	Yes	Yes	Yes	Yes
AI-Powered Threat Detection	No	No	No	Yes
Post-Quantum Cryptography	No	No	No	Yes
Blockchain-Based Auditing	No	No	No	Yes
Integration with SIEM/SOC	Yes	Yes	Yes	Yes

Table 4. Summary of comparative analysis between Rotarix and other competents

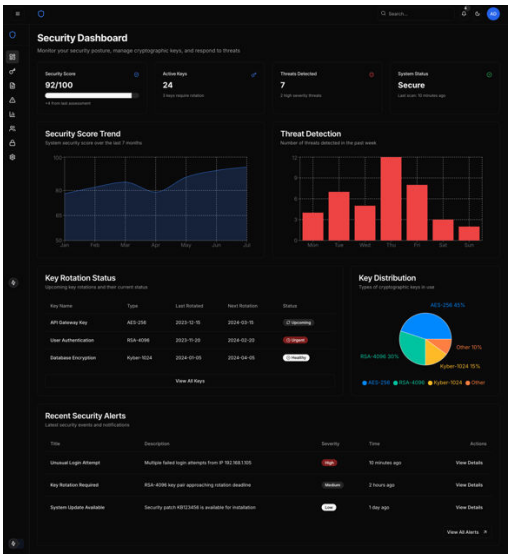
It can observed that Rotarix uniquely integrates AI-driven threat detection with post-quantum key security. While AWS and Azure provide manual key rotation, Rotarix like centralized logging in traditional KMS solutions. While AWS and Azure provide manual key rotation, Rotarix automates it based on real-time threat analysis.

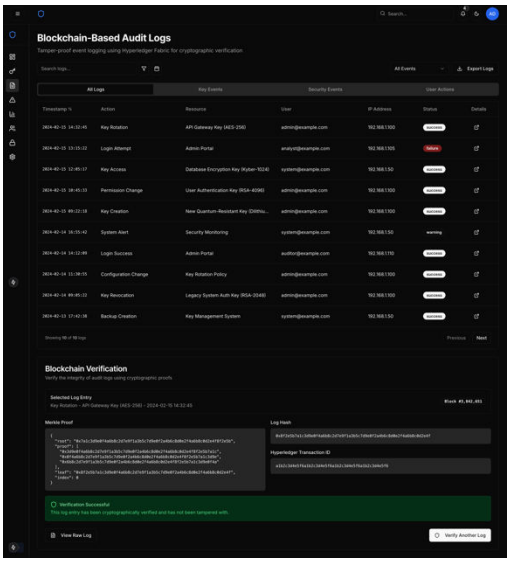
V. Conclusion

The experimental results confirm that Rotarix provides an efficient, secure, and scalable key management solution by integrating AI-driven threat detection, blockchain-backed auditing, and quantum-resistant encryption. With continued refinement and real-world testing, Rotarix based on real-time risk assessments ensures minimal disruption while maintaining high-security guarantees. The results demonstrate that Rotarix is not only effective in identifying potential

security threats but also capable of executing rapid and secure cryptographic key updates without compromising system performance.

The AI-driven anomaly detection model has exhibited strong accuracy, achieving an F1-score of 92.3%, ensuring reliable detection of security threats while minimizing false positives. Scalability tests confirm that the system operates efficiently under high computational loads, making it suitable for enterprise-scale security infrastructures. Additionally, blockchain integration for logging key rotation events introduces a 300ms delay, which is a minor trade-off for ensuring tamper-proof security and auditability. Furthermore, the implementation of Kyber and Dilithium quantum-resistant encryption algorithms enhances the system's resilience against future cryptographic threats posed by quantum computing advancements.





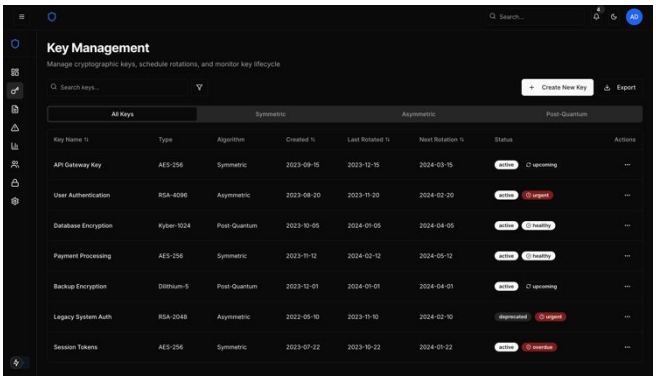


Figure 3. Few Screenshots of Rotarix Dashboard.

Despite its advantages, Rotarix still faces certain limitations that warrant further research and optimizations. The primary concern is the latency introduced by blockchain-based logging, which, while providing transparency and immutability, slightly impacts real-time performance. Future optimizations could involve batch processing of event logs to reduce write overhead without compromising auditability. Additionally, while the current AI model achieves high detection accuracy, leveraging federated learning across distributed infrastructures could further refine its ability to identify security threats in diverse environments. Another promising direction for improvement lies in adaptive cryptographic policies, where key rotation intervals are dynamically adjusted based on risk levels, ensuring optimal security while minimizing unnecessary computational overhead.

Building upon this foundation, future work will focus on deploying Rotarix in real-world enterprise environments to assess its effectiveness in handling live security incidents. Additionally, integrating the system with existing SIEM (Security Information and Event Management) and SOC (Security Operations Center) platforms will enhance its interoperability and adoption in industry settings. Further exploration into post-quantum cryptographic alternatives will also be a priority to ensure long-term cryptographic resilience against emerging attack vectors.

In conclusion, Rotarix represents a significant advancement in automated cryptographic key management by bridging AI-driven anomaly detection, blockchain-based transparency, and quantum-resistant encryption techniques. Its ability to provide autonomous, real-time security enforcement while maintaining high efficiency and auditability makes it a compelling solution for modern cybersecurity challenges. With continued refinement and real-world testing, Rotarix has the potential to set new standards in cryptographic key lifecycle management for enterprise security.

REFERENCES

1. Everspaugh, A., Paterson, K., Ristenpart, T., & Scott, S. (2017). Key Rotation for Authenticated Encryption. Advances in Cryptology – CRYPTO 2017, 98–129. https://doi.org/10.1007/978-3-319-63697-9_4
2. Fang, X., Zheng, L., Fang, X., Chen, W., Fang, K., Yin, L., & Zhu, H. (2024). Pioneering Advanced Security Solutions for Reinforcement Learning-Based Adaptive Key Rotation in Zigbee Networks. Scientific Reports, 14, Article 13931. https://doi.org/10.1038/s41598-024-64895-8

3. Amazon Web Services. (n.d.). Rotating AWS KMS keys. In AWS Key Management Service Developer Guide. Retrieved March 28, 2025, from https://docs.aws.amazon.com/kms/latest/developerguide/rotating-keys-enable.html

4. Amazon Web Services. (n.d.). Rotating AWS KMS keys on demand. In AWS Key Management Service Developer Guide. Retrieved March 28, 2025, from https://docs.aws.amazon.com/kms/latest/developerguide/rotating-keys-on-demand.html