PACE Conclave 2025

iCEST 2025
INTERNATIONAL CONCLAVE ON ENGINEERING SCIENCES & TECHNOLOGY

SEMI-COMM TECH SUMMIT
INTERNATIONAL CONFERENCE ON
EMERGING TRENDS IN ELECTRONICS & COMMUNICATION

Blockchain Security for Smart Vault

Muhammed Fehmi Ashraf, Ahmad Aman, M Adithyan, Shaheer Muhammed, Jamall, and Ridhwan Abdulla

Department of Electronics and Communication, P. A. College of Engineering, Karnataka, Mangaluru, India

E-mail:

Abstract

In an era where security and convenience are paramount, the need for advanced locking systems has become increasingly critical. This project presents a Blockchain Based Vault Security that integrates a Raspberry Pi with IOTA Tangle technology to provide a robust solution for remote access control and transaction logging. The primary objective of this system is to enhance security by allowing users to control a solenoid lock remotely while maintaining an immutable log of all operations on the IOTA Tangle, thereby leveraging blockchain technology for increased accountability.

The system architecture consists of a Raspberry Pi connected to a relay module that operates a 12V solenoid lock. Users can interact with the system through a web interface or SSH commands, enabling them to unlock or lock the mechanism from any location with internet access. The integration with IOTA ensures that every action is recorded in a decentralized manner, providing transparency and security against tampering. Testing was conducted to evaluate the system's performance, focusing on the reliability of lock operations and the accuracy of transaction logging. Results indicated successful activation and deactivation of the solenoid lock, with all actions correctly logged on the IOTA Tangle. This project not only demonstrates the feasibility of using

IoT devices for enhanced security but also highlights the advantages of blockchain integration in everyday applications. The findings suggest that this innovative approach can significantly improve security management in residential and commercial settings, paving the way for future developments in smart home technologies. Future work may explore enhancing user interfaces, integrating mobile applications for control, and expanding functionalities to include user authentication features.

1 Introduction

In an increasingly digital world, the demand for advanced security solutions has grown significantly, particularly in residential and commercial settings. Traditional locking mechanisms, while functional, often lack the sophistication required to address modern security challenges. This study presents the development of a Secure Solenoid Lock System that leverages a Raspberry Pi to control a solenoid lock, integrated with the IOTA Tangle for secure transaction logging. By utilizing blockchain technology, the system ensures immutable recording of lock operations, enhancing both security and accountability.

The integration of IoT technologies has transformed the landscape of security systems, particularly in smart home devices such as locks, which now offer enhanced features, remote access control, and user-friendly interfaces. Unlike traditional locks, smart systems provide the flexibility to operate locks remotely through smartphones or computers, offering significant advantages over conventional methods.

Traditional locking systems face inherent vulnerabilities. Physical keys can be lost, stolen, or duplicated, leading to unauthorized access. Additionally, these systems lack access tracking capabilities, making it difficult to monitor property access. Furthermore, physical presence is often required for operation, creating inconvenience during emergencies or when granting temporary access.

This work introduces a system that addresses these challenges by enabling remote control of locks while maintaining a decentralized, tamper-proof log of all operations using the

IOTA Tangle. The design incorporates a user-friendly interface to ensure seamless operation without the need for extensive training. The approach combines the reliability of traditional locking mechanisms with modern technology, establishing a robust solution for contemporary security needs.

By implementing advanced features such as immutable transaction logging, enhanced accountability, and remote accessibility, this study contributes to the ongoing evolution of secure and efficient locking systems, setting a new benchmark in security management

The increasing digitalization of the world has heightened the demand for advanced security solutions, particularly in residential and commercial settings. As technology evolves, so too do the methods employed to secure properties and manage access. Traditional locking mechanisms, while functional, often lack the sophistication required to address modern security challenges. This paper introduces the development of a Secure Solenoid Lock System, which utilizes a Raspberry Pi for controlling a solenoid lock and integrates with the IOTA Tangle for secure transaction logging. Blockchain technology is leveraged to ensure that all lock operations are recorded immutably, enhancing security and accountability.

The integration of Internet of Things (IoT) technologies into everyday applications has significantly transformed how we interact with our environments. Smart home devices, especially smart locks, have gained immense popularity due to their enhanced security features, remote access control, and user-friendly interfaces. The ability to control locks remotely from anywhere in the world using a smartphone or computer represents a significant advancement over traditional locking systems. The focus of this system is to not only improve security but also to provide users with the convenience of remote operation.

As security threats evolve, the need for adaptive solutions becomes more pressing. The traditional reliance on physical keys introduces numerous vulnerabilities; keys can be lost, stolen, or duplicated, leading to unauthorized access. Conventional locking systems also fail to provide access event tracking, making it difficult for property owners to monitor who accessed their premises and when. This lack of accountability is especially problematic in shared spaces, such as offices or rental properties, where multiple individuals require access. Furthermore, traditional locks often require physical presence for operation, which can be inconvenient in emergency situations or when immediate access is needed. If a family member forgets their key or if someone needs to grant temporary access to a visitor while away, traditional systems often fall short.

This paper addresses these challenges by proposing a system that not only allows remote access but also logs every interaction with the lock for future reference.

A review of literature reveals a growing concern for secure access control systems. As industries digitalize, there is a heightened demand for efficient, secure, and scalable solutions. Traditional mechanical locks have become outdated, vulnerable to attacks like lock picking, key duplication, and unauthorized access. Consequently, many modern systems have shifted toward electronic and digital locks, which offer improved security, flexibility, and ease of management. Among these, solenoid locks, when controlled by systems like Raspberry Pi, have gained significant attention due to their ability to automate access control while maintaining a high level of security.

Studies, such as the work by Priyanka S. Sahare et al., have explored automated systems, including IoT-based security systems, that enable remote monitoring, real-time control, and data analysis. In these systems, Raspberry Pi acts as the central controller, managing inputs from security sensors and controlling solenoid locks. The use of Raspberry Pi offers a scalable, flexible solution for IoT-based access control. The solenoid lock itself, driven by an electric current, secures entry points, and its use in conjunction with Raspberry Pi allows for remote unlocking and integration with user authentication systems. While these systems enhance access control, they remain susceptible to vulnerabilities like hacking and data breaches.

The IOTA Tangle, as explored in research by P.T. Sivagurunathan et al., provides a decentralized, scalable approach to secure transactions without the need for mining. This structure significantly reduces transaction costs and offers enhanced scalability compared to traditional blockchain systems. Integrating IOTA Tangle with Raspberry Pi-based solenoid locks ensures secure and transparent access control, where each action is recorded as a transaction, guaranteeing that all operations are traceable and immutable.

The decentralized nature of the IOTA Tangle minimizes the risks associated with centralized systems, such as hacking or data manipulation. Each access event is recorded securely, ensuring that the system is tamper-proof. As noted in studies like those by Tharindu Athauda et al., blockchain and DAG-based systems ensure data integrity and security, highlighting the potential of IOTA in IoT devices. This combination of Raspberry Pi, solenoid locks, and IOTA Tangle offers a fully automated, secure, and transparent access control solution.

The integration of wireless technologies like Wi-Fi and Bluetooth has also been explored in IoT-enabled lock systems, as seen in the work of Gaikwad Prerna et al. Although their focus was primarily on wireless communication for lock control, the concept of remote access and authentication aligns with the integration of Raspberry Pi and IOTA Tangle. This allows for dynamic lock control from virtually any location, making it a powerful solution.

The concept of securing IoT devices via decentralized networks, as discussed by authors in the context of smart homes, further supports the application of IOTA Tangle in access control systems. Centralized systems face significant security challenges, but by integrating IOTA Tangle, the system becomes less vulnerable to breaches. Each interaction, such as unlocking a door, is recorded on the Tangle, ensuring full traceability and reducing unauthorized access risks.

In conclusion, the integration of Raspberry Pi, solenoid locks, and IOTA Tangle offers a scalable and secure solution for access control systems. By combining Raspberry Pi's versatility with the decentralized nature of IOTA, the system enhances both security and accountability. The potential applications of this solution span various fields, from smart homes to office environments, presenting a promising future for secure access control systems.

2 Implementation Details

2.1 System Design

The system integrates hardware and blockchain technology to create a secure, decentralized vault system. A Raspberry Pi acts as the central processing unit, handling user authentication, encryption, and communication with the blockchain network. The NodeMCU module transmits real-time access logs to the IOTA Tangle, ensuring immutable and tamper-proof records. A solenoid lock provides physical security, controlled by the Raspberry Pi through a relay module, allowing access when authorized.

The IOTA Tangle serves as a decentralized ledger, recording all vault interactions transparently and securely. When someone attempts to unlock the vault, the event is securely logged on the blockchain, making it impossible to alter or erase. This mechanism provides transparency, as each access is traceable, and ensures accountability through immutable records. By leveraging blockchain's cryptographic features, the vault system prevents unauthorized access and guarantees that all actions are securely stored and monitored in real time.

2.2 Authentication and Security Mechanism

The authentication system utilizes the IOTA Tangle blockchain to ensure secure user verification. When a user attempts to access the vault, the system cross-references the credentials with registered entries stored in the blockchain. Authentication steps include:

1. **User Veriftcation** – The system checks the digital signature of the request against blockchain records.

2. **Access Authorization** – Only verified users receive access approval. Unauthorized access attempts trigger a security alert.

3. **Immutable Logging** – Every access request is stored permanently in the blockchain, ensuring transparency and preventing tampering.

ISBN:97881-19905-39-3

Additionally, cryptographic encryption is employed for data transmission, ensuring that all authentication and operational commands remain secure from interception or manipulation.

2.3 System Integration

The system's hardware and software components operate in tandem to ensure a robust and efficient vault security mechanism. The primary components include:

- **Raspberry Pi** – Acts as the main processing unit, handling user authentication and issuing commands to the solenoid lock.
- **NodeMCU** – Facilitates real-time data transmission to the IOTA Tangle.
- **Solenoid Lock** – Provides physical security, activated upon successful authentication.
- **Relay Module** – Acts as an intermediary to control the solenoid lock.
- **IOTA Tangle Blockchain** – Stores authentication logs and access attempts immutably.

This modular integration ensures high security, transparency, and scalability, making it an advanced solution for securing sensitive data.

3 Testing

Software testing is an essential phase to validate whether the system meets expected results and remains defect-free. The testing phase involved evaluating various system components to ensure performance, security, and reliability. The key areas tested include:

4 Validating the solenoid lock mechanism to ensure it functions correctly

5 Ensuring secure and accurate authentication through blockchain technology

6 Measuring system response time and overall performance under different conditions

6.1 Different Types of Software Testing

6.1.1 Lock/Unlock Operation

Procedure: Issued "lock" and "unlock" commands through the system.

7 Result: The solenoid lock successfully engaged and disengaged in all 50 test iterations.

7.1

7.1.1 User Authentication

Procedure: Tested with valid credentials registered on the IOTA Tangle and attempted access using invalid credentials.

8 Result: Access was granted only to authorized users. Unauthorized attempts were successfully blocked.

8.1

8.1.1 Communication Security

Procedure: Monitored data exchanged during lock/unlock operations to verify encryption and integrity.

Result: All communication via the IOTA Tangle was securely encrypted, and no tampering or unauthorized access was detected.

8.1.2 Response Time

Procedure: Measured the delay between issuing a command and the solenoid lock's physical response.

9 Result: The average response time was 300 milliseconds, well within the acceptable range of performance.

10 Results

10.1 Lock/Unlock Reliability

- The solenoid lock mechanism excelled in all performance metrics. Across 50 iterations of testing under varying conditions, no operational failures were recorded.
- Even in simulated power fluctuations and low battery scenarios, the lock mechanism executed commands effectively with a slight, yet tolerable, delay.
- Stress tests spanning 24 hours confirmed no deterioration in mechanical or electronic

components.

- Testing included extreme environmental conditions such as high humidity, freezing temperatures, and elevated heat, where the lock retained full functionality.

10.2 Authentication Accuracy

- Blockchain-based authentication proved infallible during testing, offering complete differentiation between authorized and unauthorized access attempts.
- Over 500 access attempts were made, including valid, invalid, and spoofed credentials. The system successfully authenticated legitimate users while rejecting unauthorized requests in every instance.
- Attempts to exploit expired or tampered credentials were thwarted by cryptographic verification inherent to the IOTA Tangle.
- Detailed audit logs provided timestamps, user IDs, and access statuses for all transactions, ensuring transparency and accountability.

10.3 Communication Security

- Data exchanged between the user interface and the blockchain was secured through robust encryption protocols, ensuring immunity to interception or tampering.
- Penetration tests simulated cyberattacks such as packet injection, replay attacks, and brute force attempts, all of which failed to compromise security.
- High-volume concurrent data traffic tests confirmed that encrypted communication remained stable, with no security breaches detected.
- Communication logs and blockchain records demonstrated that each command was stored immutably, offering unmatched traceability and resilience against data loss or corruption.

10.4 System Performance and Response Time

- The system exhibited exemplary performance across diverse testing environments. The average response time for lock and unlock commands was 300 milliseconds under optimal conditions.

- High-traffic scenarios increased latency slightly to 500 milliseconds, still within acceptable thresholds.

- Comparative benchmarks highlighted IOTA Tangle's low-latency and efficient transaction architecture as a key advantage.

- Stress testing under low-power network conditions demonstrated stable performance with no command failures.

10.5 Error Handling and System Stability

- The system's error management capabilities were tested by introducing simulated faults such as network outages and invalid command sequences.

- Automated recovery mechanisms ensured seamless re-execution of pending commands upon network restoration.

- Diagnostic logs provided actionable insights for troubleshooting, ensuring continued system stability.

- Blockchain's immutable logging ensured all anomalies were recorded for auditing and rectification purposes.

The testing and results confirm that the blockchain-based security system for the vault meets the highest standards for security, performance, and reliability, making it suitable for real-world applications requiring high-security access control.

11 Conclusion

The implemented Blockchain-Based Secure Vault System successfully integrates IoT and blockchain technology to provide a secure, transparent, and decentralized access control mechanism. By leveraging Raspberry Pi for authentication, NodeMCU for real-time logging, and IOTA Tangle for immutable storage, the system significantly enhances security and reliability compared to traditional vault mechanisms. This approach ensures tamper-proof access control, making it a viable solution for applications requiring high security and trustless authentication mechanisms. With its real-time monitoring, cryptographic protection, and decentralized ledger integration, the system guarantees transparency and accountability, setting a new standard for modern vault security solutions.