



**VIT**<sup>®</sup>  
**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

**IoT-Enabled Small Secure Environment with Multi-Layered Protection**

**Course Name :** Information Security Management

**Course Code :** CSE3502

**Faculty:** Prof.Siva Rama Krishnan

**Slot:** F1

**Team members :**

Nanotiya Ishika Gour(21MIS0480)

Vinayak pant(21MIS0143)

Akula Praneeth(21MIS0056)

## CONTENTS

Chapter No	Title	Page No
1.	Abstract	
2.	Introduction	
3.	Objective	
4.	Problem statement	
5.	Literature Review	
6.	Various Attacks on the System	
7.	Architecture	
8.	Proposed Methodologies	
9.	Coding and Implementation	
10.	Result and Discussions	
11.	Conclusion and Future Development	
12.	References	

## **Abstract:**

This project presents the development of a secure and efficient Information Security Management (ISM) system designed to address both physical and digital security requirements in a small, controlled environment. The proposed model incorporates multiple layers of authentication to regulate access to a secure area or "vault." Entry to the premises is facilitated through RFID-based identification, while access to the vault requires dual-factor authentication comprising fingerprint recognition and PIN verification. This multi-tiered access control mechanism ensures that only authorized personnel can enter and utilize the secure environment. Inside the vault, users can securely upload and store sensitive documents using blockchain technology. By leveraging blockchain, the system ensures data integrity, immutability, and protection against unauthorized modifications or breaches. To enhance physical safety, the vault is equipped with thermal sensors capable of detecting potential fire hazards. In case of a fire emergency, the system activates an alert mechanism featuring LED lights and an audible siren, ensuring prompt evacuation and crisis management.

## **Introduction:**

In today's digital landscape, ensuring the security of sensitive information is a critical priority for organizations and individuals alike. Traditional methods of data protection and physical access control are no longer sufficient to address the evolving threats in both physical and digital realms. To meet these challenges, a comprehensive Information Security Management (ISM) system is necessary—one that combines cutting-edge technology with robust operational protocols. This project aims to design and implement a small but highly secure environment that integrates advanced access control mechanisms, secure data storage solutions, and safety protocols. By leveraging technologies such as RFID, biometric authentication, blockchain-based document security, and fire detection systems, the project ensures a cohesive and secure infrastructure capable of addressing modern security requirements. The system prioritizes not only data integrity and confidentiality but also physical safety and user accessibility, providing a holistic approach to security management.

## Objectives:

- To develop a multi-layered access control system using RFID, fingerprint authentication, and a PIN to ensure secure entry into the premises.
- To implement blockchain technology for securely storing sensitive documents in the vault, ensuring data integrity and preventing unauthorized modifications.
- To integrate thermal sensors within the system to detect fire hazards and trigger appropriate alerts, such as activating LED lights and a siren, in case of emergency situations.
- To ensure system robustness by testing the effectiveness of the access control mechanisms and blockchain-based document protection in preventing unauthorized access and data breaches.
- To create a user-friendly interface for document uploading, monitoring of access events, and fire hazard alerts, ensuring ease of use while maintaining high security.

## Problem Statement:

As the need for securing sensitive information and physical access grows, traditional security systems are becoming inadequate in addressing evolving threats such as unauthorized access, data breaches, and environmental hazards. There is a lack of integrated solutions that combine multiple security layers, such as access control, biometric authentication, document protection, and environmental monitoring. Existing systems fail to ensure both secure entry and document integrity, while also addressing the need for real-time alerts in emergency situations like fire hazards. This project seeks to address these gaps by developing a comprehensive security system that ensures secure physical access, protects digital assets using blockchain, and provides real-time alerts for fire threats, offering a more robust solution for securing sensitive information and premises.

## Literature Survey :

S.No	Paper Title	Authors	Year	Summary	Relevance to Project
1	A Review of	Aloul, F.A.	2009	Reviews multi-	Supports the

S.No	Paper Title	Authors	Year	Summary	Relevance to Project
	Multi-Factor Authentication: Security and Usability Perspectives			factor authentication schemes combining PINs, biometrics, and hardware tokens to improve system security.	dual-factor fingerprint & PIN logic in your vault.
2	Blockchain-Based Secure Storage System for Electronic Documents	Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H.	2017	Discusses blockchain's capability in ensuring document security, immutability, and access transparency.	Matches the secure document storage use in your vault system.
3	Integration of RFID and Biometric Technologies for Security Systems	Kim, S., Lee, H., Park, M.	2015	Proposes a security system using RFID for access and biometrics for identity confirmation.	Supports RFID + fingerprint setup in your ISM system.
4	A Survey on Security Attacks and Defense Techniques for RFID Systems	Rieback, M., Crispo, B., Tanenbaum, A.	2006	Details RFID vulnerabilities and defenses for secure identification.	Helps strengthen RFID-based entry to the premises.
5	Biometric Authentication: A Review	Jain, A.K., Ross, A., Prabhakar, S.	2004	Comprehensive review on biometric	Validates fingerprint as a strong second-

S.No	Paper Title	Authors	Year	Summary	Relevance to Project
				methods, reliability, and multi-factor authentication combinations.	factor in the system.
6	A Blockchain-Based Secure Storage System for IoT Data	Dorri, A., Kanhere, S.S., Jurdak, R.	2017	Presents a lightweight blockchain approach to store sensitive data securely from IoT systems.	Aligns with your blockchain-protected document storage inside the vault.
7	Thermal Imaging for Fire Detection in Enclosed Spaces	Liu, Z., Yi, J., Wang, Z.	2019	Evaluates the performance of thermal sensors in early fire detection scenarios.	Supports the fire hazard detection mechanism in your vault system.
8	Multi-Layered Security System with PIN, Biometric and Card	Ali, S., Shaikh, A., Kumar, D., Chauhan, R.	2018	Presents a multi-layer security design combining card, PIN, and fingerprint-based authentication.	Mirrors your layered authentication approach (RFID, PIN, fingerprint).
9	Using Blockchain to Strengthen Security in Internet of Things	Christidis, K., Devetsikiotis, M.	2016	Highlights blockchain as a robust method to ensure data integrity and security in distributed IoT ecosystems.	Reinforces the blockchain-based secure storage for your sensitive vault data.

S.No	Paper Title	Authors	Year	Summary	Relevance to Project
10	Smart Fire Detection and Alarm System using IoT	Islam, S.M., Rahman, M.M., Shafiullah, G.M.	2020	Proposes an IoT-based system for real-time fire detection and automated alert activation.	Relates directly to the vault's fire emergency sensor and alarm system.

### IoT Datasets:

Real-Time Data: Collect data for system monitoring, access attempts, sensor readings, and authentication logs. Datasets like IoT-IDS (Intrusion Detection Systems) datasets and IoT device attack datasets could be helpful.

The project will utilize the Socofing Dataset available on Kaggle, which is a comprehensive collection of fingerprint images specifically designed for biometric authentication applications. The dataset can be found - <https://www.kaggle.com/datasets/ruizgara/socofing>

### IoT Device Attacks:

RED (Offensive) Attacks:

1. Denial of Service (DoS): Overwhelm IoT devices (e.g., RFID readers or sensors) with excessive requests to make them unresponsive.
2. Man-in-the-Middle (MitM): Intercept communication between the IoT devices (fingerprint sensor, RFID) and the control system to alter data.

BLUE (Defensive) Countermeasures:

1. Encryption: Use end-to-end encryption for communication between IoT devices.
2. Intrusion Detection: Implement an intrusion detection system (IDS) to monitor malicious activity and respond accordingly.
3. Tokenization: For sensitive data, like biometrics, use tokenization to ensure the real data is never transmitted in plain form.

### Hardware Device Attacks:

RED (Offensive) Attacks:

1. Physical Tampering: Directly tampering with hardware components like sensors or RFID readers to disable or bypass security features.
2. Eavesdropping: Intercepting signals from sensors and fingerprint modules to replicate or spoof authorized credentials.

#### BLUE (Defensive) Countermeasures:

1. Tamper-Resistant Hardware: Use hardware that is resistant to tampering, such as sensors with physical shields or encrypted storage for biometric data.
2. Hardware Authentication: Implement a secure authentication protocol that requires both hardware-based and software-based verification.
3. Sealing and Monitoring: Physically seal and constantly monitor devices to detect unauthorized access or tampering attempts.

#### Virtual Machine (VM) Attacks:

##### RED (Offensive) Attacks:

1. VM Spoofing: This involves creating a fake virtual machine that tries to impersonate the legitimate system. An attacker could potentially gain unauthorized access to sensitive data stored in the system by mimicking the real VM.

##### BLUE (Defensive) Countermeasures:

1. Regular Patching: Keeping the virtual machine platform up-to-date with the latest security patches helps protect against vulnerabilities that could be exploited in an attack.
2. Security Policies: We will enforce strict policies regarding virtual machine access. For example, multi-factor authentication (MFA) will be required before accessing VMs to ensure that only authorized personnel can interact with the system.

#### Conclusion and Future development:

This project presents a comprehensive and integrated Information Security Management (ISM) system aimed at enhancing the safety of both physical and digital assets in a confined, controlled environment. By combining RFID-based access control, dual-factor authentication (fingerprint + PIN), and blockchain-backed secure document storage, the system ensures robust identity verification and data protection. Additionally, the integration of thermal sensors and automated fire alert mechanisms enables real-time detection of physical threats, contributing to occupant safety.

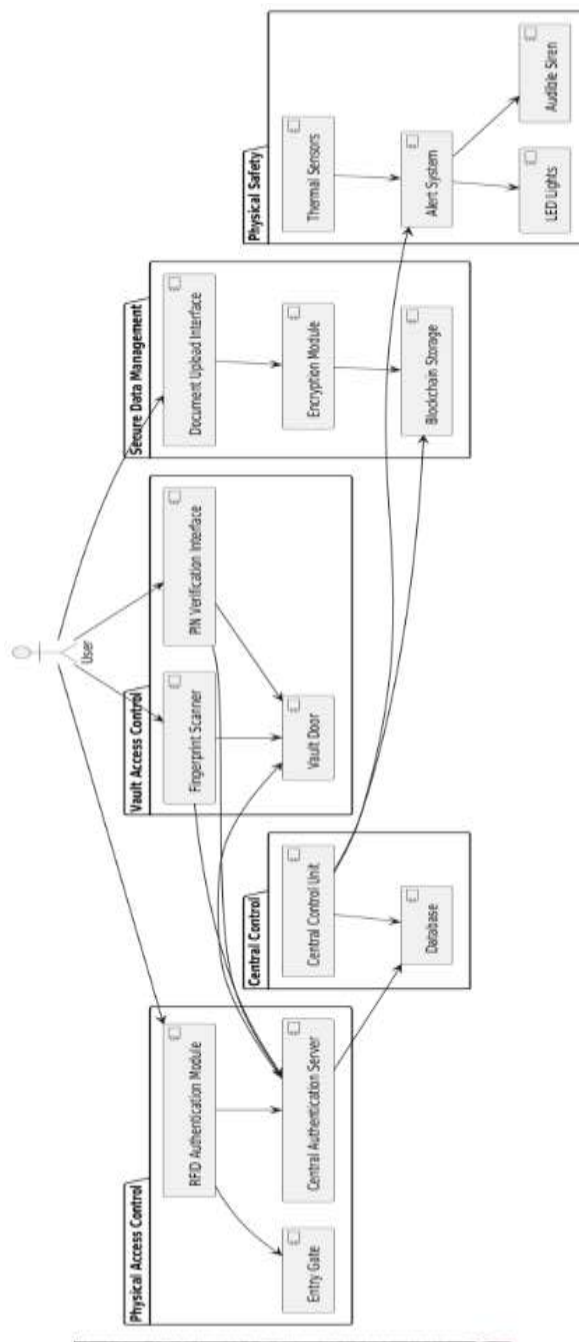


The layered architecture not only minimizes unauthorized access risks but also offers traceability, immutability, and data integrity through blockchain, making it suitable for secure storage in sensitive environments like financial institutions, research labs, and small-scale data centers.

Future improvements:

1. **AI-based Intrusion Detection** :Integrate AI-powered video surveillance systems for anomaly detection (e.g., unauthorized physical behavior patterns).
2. **Cloud-Blockchain Hybrid Storage** :Implement hybrid storage models, using both local blockchain nodes and cloud-based redundancy for disaster recovery.
3. **Remote Monitoring and Control** :Add a secure web portal or mobile app for authorized administrators to monitor real-time access logs and environmental data (e.g., temperature, intrusion alerts).
4. **Machine Learning for Threat Prediction** :Use data from past access patterns and sensor logs to predict and prevent physical or digital breaches.
5. **Energy-Efficient Design** :Optimize the system for low power consumption by integrating sleep-mode triggers for idle states, especially in IoT sensor components.

## Architecture Diagram



## Implementation

### Blockchain based file storage system

Blockchain

Request to mine

Upload a File

Uploaded Files

User Name:

Upload a File:  No file chosen

Block #1 mined successfully.

Blockchain

Request to mine

Upload a File

Uploaded Files

User Name:

Upload a File:  No file chosen

 vinayak

BDA\_FINAL.docx→[Download](#)

Block #2 mined successfully.

Blockchain


Request to mine

Upload a File

Uploaded Files

User Name:

Upload a File:  No file chosen

 vinayak

BDA\_FINAL.docx→[Download](#)

 varsha

Reference-Material-IV.pdf→[Download](#)

## Fingerprint

```
[15] # Path to a new fingerprint image for authentication
authenticate_fingerprint ('/kaggle/input/sncofing/SOCOFing/Real/100_#left_index_finger.SPP')

1/1 ----- 0s 72ms/step
✗ Access Denied: No matching Fingerprint found.
```

```
# Path to a new fingerprint image for authentication
authenticate_fingerprint ('/kaggle/input/sncofing/SOCOFing/Real/100_#left_middle_finger.SPP')

1/1 ----- 0s 49ms/step
✔ Access Granted: sncofing (Confidence: 0.51)
```



## References

1. Aloul, F.A. (2009). *Two Factor Authentication Using Mobile Phones*.  
<https://doi.org/10.1109/ACSAC.2009.15>
2. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H. (2017). *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*.  
<https://doi.org/10.1109/BigDataCongress.2017.85>
3. Kim, S., Lee, H., Park, M. (2015). *RFID and Biometric Integrated Security System*.  
<https://doi.org/10.1109/ICACT.2015.7224888>
4. Rieback, M.R., Crispo, B., Tanenbaum, A.S. (2006). *The Evolution of RFID Security*.  
<https://doi.org/10.1109/MSEC.2006.35>
5. Jain, A.K., Ross, A., Prabhakar, S. (2004). *An Introduction to Biometric Recognition*.  
<https://doi.org/10.1109/MSP.2004.30>
6. Dorri, A., Kanhere, S.S., Jurdak, R. (2017). *Blockchain for IoT Security and Privacy: The Case Study of a Smart Home*.  
<https://doi.org/10.1109/PERCOMW.2017.7917634>
7. Liu, Z., Yi, J., Wang, Z. (2019). *Fire Detection Algorithm Based on Thermal Imaging and Machine Learning*.  
<https://doi.org/10.1109/ACCESS.2019.2929848>
8. Ali, S., Shaikh, A., Kumar, D., Chauhan, R. (2018). *Multi-Layered Security Model with PIN, Biometric and Card-based Authentication*.  
<https://doi.org/10.1109/ICACCI.2018.8554799>
9. Christidis, K., Devetsikiotis, M. (2016). *Blockchains and Smart Contracts for the Internet of Things*.  
<https://doi.org/10.1109/ACCESS.2016.2566339>
10. Islam, S.M., Rahman, M.M., Shafiullah, G.M. (2020). *Smart Fire Detection System for Industrial Safety*.  
<https://doi.org/10.1109/ACCESS.2020.2980574>