

**EIA3010 ACADEMIC RESEARCH**

**SECURING SMART INVENTORY MANAGEMENT SYSTEMS:  
A REVIEW OF CYBERSECURITY APPROACHES AND CHALLENGES**

**NUR NABILAH BINTI NORANIZAM  
(22061479)**

**FACULTY OF BUSINESS AND ECONOMICS  
UNIVERSITI MALAYA**

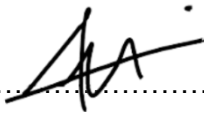
**SUBMITTED IN PARTIAL FULFILLMENT OF  
THE REQUIREMENTS FOR THE DEGREE  
OF BACHELOR OF ECONOMICS**

**SESSION 2024/2025**

## DECLARATION OF ORIGINALITY OF WORK

I admit that this Academic Research is my own work except the information, excerpts and references used have been acknowledged. I also admit that the contents of the Academic Research are original and have not been submitted to the Universiti Malaya or other institutions for any other purposes. I am solely responsible for all the contents of this Academic Research. Faculty of Business and Economics and Universiti Malaya shall be absolved from any form of legal actions arising from this research.

Signature: .....



Name: NUR NABILAH BINTI NORANIZAM

Matric No.: 22061479

Date: 23 June 2025

## **ACKNOWLEDGEMENTS**

I am truly grateful to my supervisor, Dr. Elayaraja A/L Aruchunan, for his unwavering support, valuable feedback, and expert guidance that have played a crucial role in my research journey. His guidance assisted me in exploring new and unfamiliar areas.

I would like to extend my heartfelt gratitude to my final year project group members: Zhang Hao Zhe, Jazzlyn Ling Xin Hui, Ong Xiao Xuen and Muhammad Ammar Bin Robings. Their collaboration, technical insight, and dedication made the development of the application an enriching and rewarding experience. I truly appreciate the support and guidance I got while working on the app.

I want to express my gratitude to my close friends: Ee Ren, Aqilah and Kuganaa, who have supported me, especially during my endless complaints. Your presence has made this journey feel less overwhelming and much more significant.

Finally, I want to express my gratitude to the quiet companions who helped me stay grounded during those long nights of writing and debugging. Thank you for being a part of this unforgettable journey. This research journey has been filled with valuable lessons, and I sincerely appreciate everyone who played a part, whether directly or indirectly, in bringing it to fruition.

## ABSTRACT

Smart inventory system has advanced significantly over the years which greatly improved operational efficiency. However, these rapid developments have also introduced new and improved cybersecurity attacks involving data breaches, ransomware and insider threats. This study aims to develop an application-level framework for secure smart inventory systems, to implement key cybersecurity features, and to examine the performance of these features in practical settings. A literature review is conducted using Scopus, the university library's database and Google Scholar with publication dated to 10 years back. Findings show that encryption, zero-trust networks and AI-based monitoring are widely used, though many studies did not explicitly test these methods' performance or its compliance with established cybersecurity standards and frameworks. Therefore, further real-world testing and validation are necessary to ensure both effectiveness and regulatory abidance in future implementations.

Keywords: Cybersecurity, Inventory Management, Inventory System, Smart Inventory System, Application Security

## TABLE OF CONTENTS

List of Tables .....	i
Acronyms .....	ii
1.0 Introduction .....	1
1.1 Background of Study .....	1
1.2 Problem Statement.....	1
1.3 Research Questions .....	2
1.4 Research Objectives .....	2
1.5 Research Hypothesis .....	3
1.6 Scope of the Research and the Limitations .....	3
1.7 Significance of the Research.....	4
1.8 Outline of the Report .....	4
2.0 Literature Review .....	5
2.1 Resources, Materials and Tools .....	5
2.2 Literature Review Analysis .....	7
3.0 Methodology .....	20
3.1 Features to Implement .....	21
3.2 Approach to Implementation.....	23
3.3 Impact on Application Security .....	23
3.4 Integration with Security Frameworks.....	26
4.0 Conclusion and Recommendations.....	27
4.1 Summary of Findings .....	27
4.2 Answering to Objectives.....	28
4.3 Implications .....	28
4.4 Limitation of the Research.....	30
4.5 Suggestions for Future Research .....	31
5.0 Reference .....	34
6.0 Appendices .....	38

## **List of Tables**

Table 1: Strengths and Weaknesses of Key Security Technologies for SIMS

## **Acronyms**

### **A**

AI – Artificial Intelligence

API – Application Programming Interface

### **C**

COBIT – Control Objectives for Information and Related Technologies

CRUD – Create, Read, Update, Delete

### **E**

ERP – Enterprise Resource Planning

ETSI – European Telecommunications Standards Institute

### **G**

GDPR – General Data Protection Regulation

### **H**

HTTP - Hypertext Transfer Protocol

### **I**

IDS – Intrusion Detection System

IoT – Internet of Things

ISO – International Organization for Standardization

ISMS – Information Security Management System

IT – Information Technology

### **J**

JWT – JSON Web Token

### **L**

LLM – Large Language Model

### **M**

MFA – Multi-Factor Authentication

MQTT – Message Queuing Telemetry Transport

## **O**

OCR – Optical Character Recognition

OAuth – Open Authorization

## **P**

PWA – Progressive Web App

## **Q**

QA – Quality Assurance

QR – Quick Response (as in QR code)

## **R**

RBAC – Role-Based Access Control

REST – Representational State Transfer

RFID – Radio-Frequency Identification

RLS – Row-Level Security

## **S**

SIEM – Security Information and Event Management

SIMS – Smart Inventory Management Systems

SME – Small and Medium-sized Enterprise

SQL – Structured Query Language

SSL – Secure Sockets Layer (referred via TLS)

## **T**

TLS – Transport Layer Security

## **U**

UI – User Interface

UX – User Experience

## **V**

VM – Virtual Machine

## **W**

WMS – Warehouse Management System



## **Z**

ZTA – Zero Trust Architecture

## **1.0 Introduction**

### **1.1 Background of Study**

Smart Inventory Management Systems (SIMS) mark a significant advancement in how we handle stock, logistics, and supply chains. Integrating Internet of Things (IoT) sensors, Artificial Intelligence (AI), cloud computing, and process automation allows SIMS to help organizations gain real-time visibility, predictive analytics, and improved operational efficiency. More and more sectors like manufacturing, healthcare, retail, environmental management, and public services are adopting these systems because they help reduce human error, prevent stockouts and make decision-making more efficient.

As inventory management evolves to become more digital and interconnected, the cybersecurity of SIMS has emerged as a critical issue. Digitising inventory processes introduces risks including unauthorised access, data manipulation, ransomware attacks, insider threats, and vulnerabilities associated with IoT devices. Studies conducted by Mamani et al. (2022) and Al Kurdi et al. (2022) underscore the increasing dependence on SIMS among governmental organisations and commercial enterprises. Alarming, several systems exhibit inadequate security protocols. For instance, they may fail to implement multi-factor authentication for users or to encrypt critical data by default.

Moreover, a limited number of studies have investigated SIMS deployments in relation to established cybersecurity standards such as ISO/IEC 27001 or NIST SP 800-53. The absence of standardised, validated security frameworks complicates organisations' ability to assess the maturity or security of their inventory systems. This study's basis is based on the conflict between the efficiency improvements offered by smart inventory technology and the new security problems they introduce. It provides the framework for investigating the effective security of SIMS without undermining their usefulness.

### **1.2 Problem Statement**

Despite the rapid implementation of smart inventory platforms, several firms continue to encounter substantial cybersecurity and operational difficulties stemming from antiquated practices or insufficient protection in existing systems. Current inventory programs often exhibit subpar user experience and lack essential functionalities, like real-time stock monitoring, streamlined item entry and immediate support or

assistance. These deficiencies, coupled with inadequate security measures, render systems susceptible to cyberattacks and data inaccuracies. The intricate nature and significant learning curves of most corporate inventory solutions render them daunting for adoption, particularly for Small and Medium-sized Enterprises (SMEs) with constrained IT proficiency. The market is deficient in a straightforward, visually coherent, and secure inventory management solution that prioritises automation and robust cybersecurity. Rectifying this deficiency is crucial for empowering organisations to enhance inventory precision, make informed choices, and safeguard their assets in an increasingly digital and threat-laden landscape.

### **1.3 Research Questions**

To tackle the problem stated above, this study is guided by the following research questions:

1. What components should be included in an effective application-level cybersecurity framework for SIMS to ensure data integrity, confidentiality and availability?
2. How can key cybersecurity features such as encryption, MFA, Role-Based Access Control (RBAC) and blockchain can be effectively implemented within SIMS to prevent unauthorized access and secure inventory operations?
3. How do the implemented cybersecurity features perform in practice, and to what extent do they comply with recognized regulatory and security standards?

### **1.4 Research Objectives**

Based on the questions above, the research aims to achieve the following objectives:

1. To develop an application-level cybersecurity framework tailored specifically for SIMS to ensure system integrity, confidentiality, and resilience.
2. To implement key cybersecurity features such as encryption, MFA, RBAC and blockchain for secure inventory tracking and user authentication.
3. To evaluate the performance and regulatory compliance of these cybersecurity features against established standards through simulated environments and use-case benchmarking.

## **1.5 Research Hypothesis**

This study is guided by the following hypotheses:

H1: The development of an application-level cybersecurity framework tailored for SIMS will significantly enhance integrity, confidentiality and availability of data.

H2: The implementation of cybersecurity features will effectively reduce the risk of unauthorized access and data breaches in SIMS.

H3: The implemented cybersecurity framework and features will demonstrate measurable compliance with international standards. Thereby, validating their regulatory soundness and operational effectiveness.

## **1.6 Scope of the Research and the Limitations**

This research centres on the design, development, and assessment of a secure smart inventory management application specifically designed for personal use and SMEs. This analysis focusses on the integration of essential cybersecurity features, namely encryption, MFA, role-based access control, and blockchain-based audit trails—at the application level to safeguard inventory data. The established security architecture is assessed for its capacity to maintain data integrity, confidentiality, and system resilience against attacks. Additionally, the research evaluates the alignment of these security aspects with international standards such as ISO/IEC 27001 and NIST SP 800-53, assessing the framework's compliance and resilience.

While the study covers a broad range of use cases, spanning retail, healthcare, municipal services and more, it has certain limitations. The prototype security features are implemented and tested in a simulated or controlled environment, which may not capture all the complexities and unpredictable threat vectors of real-world deployment. Due to time and resource constraints, the project could not perform industry specific implementations or long-term field testing in multiple organizations. Thus, user behavior aspects, insider threats, and long-term adaptation of the system were not fully observed. Additionally, although the security framework is designed in line with global standards, the project did not deeply explore organizational factors such as policy enforcement, ongoing cybersecurity training for staff, or detailed cost-benefit analysis of the security measures. These factors are essential for practical implementation and sustainability but fall outside the immediate scope of this student

project. Acknowledging these limitations, the findings and evaluations are positioned as preliminary steps that would benefit from future expansion and real-world validation

### **1.7 Significance of the Research**

This study is significant because it addresses the urgent need to enhance the security of Smart Inventory Management Systems, which play a crucial role in modern supply chains and business operations. As SIMS increasingly incorporate IoT devices, cloud services, and AI, they also expand the potential attack surface for cyber threats. A successful attack on an inventory system can lead to severe economic and operational consequences. For example, supply chain disruptions, lost sales due to stockouts or overstocking, theft of valuable inventory data, or regulatory penalties from data breaches. By developing and evaluating a customized application-level cybersecurity framework for SIMS, this research contributes practical solutions to mitigate those risks and maintain operational continuity.

Beyond protecting inventory data and infrastructure, this study provides practical guidance on implementing cybersecurity features in an inventory application in accordance with international standards. The intention is that a well-secured SIMS not only protects assets but also boosts business resilience and stakeholder confidence. For instance, a company that knows its inventory system is secure-by-design can operate with less fear of downtime from ransomware or unauthorized modifications of stock records. In the broader perspective, such security enhances economic stability by preventing losses and ensuring that supply chains run smoothly even in the face of cyber threats. The outcomes of this research are valuable for system designers and IT managers, offering a scalable, standards-compliant model for building security into inventory systems from the ground up (rather than as an afterthought). It also provides insights for policymakers or industry bodies interested in frameworks for improving cybersecurity in SME contexts, demonstrating that advanced security can be achieved with open-source technologies and cloud services without prohibitive cost or complexity.

### **1.8 Outline of the Report**

The remainder of this report is structured as follows: Chapter 2 presents a literature review of relevant work and concepts, examining key cybersecurity threats and countermeasures related to inventory systems. This includes technologies and approaches like blockchain, MFA, RBAC, encryption techniques, AI-driven threat

detection, and compliance with security standards. Gaps in the current literature are identified to highlight the need for this research. Chapter 3 describes the methodology and system design for the project. It details the development environment, the specific security features implemented in the prototype application, the architectural design of the system, and the testing procedures. A project timeline is also provided to outline the sequence of development activities. Chapter 4 provides the conclusion and recommendations. It summarizes the findings, discusses how the research objectives were met, notes the implications of the work, addresses limitations, and offers suggestions for future research and improvements. Finally, references and appendices are provided to support the content of the report.

## **2.0 Literature Review**

### **2.1 Resources, Materials and Tools**

To ensure that this research is grounded in credible and up-to-date knowledge, a structured literature review was conducted using a clearly defined search strategy. The aim was to gather peer-reviewed studies and authoritative sources that discuss both the technological components of SIMS and the cybersecurity approaches applied to protect such systems.

#### **2.1.1 Research Database**

The literature search utilized a range of academic databases and digital libraries, including Scopus, the Universiti Malaya Library's online repository, Google Scholar, IEEE Xplore, ScienceDirect, JSTOR, and ResearchGate. These platforms collectively cover a broad spectrum of relevant disciplines, ensuring a comprehensive collection of sources related to smart inventory systems and cybersecurity.

#### **2.1.2 Search Strategy**

A systematic search strategy was employed using combinations of keywords and Boolean operators. Two primary thematic clusters of keywords were used.

The first cluster targeted smart inventory systems, using terms like "smart inventory system," "smart inventory management," "digital inventory," "automated inventory," and "inventory control system."

The second cluster targeted cybersecurity and protection mechanisms, with terms such as "cybersecurity," "information security," "data protection," "authentication,"

“authorization,” “RBAC,” “MFA,” “encryption,” “blockchain,” “smart contracts,” “IDS” (Intrusion Detection System), “zero trust architecture,” “TLS,” “OAuth,” and “secure API.”

Advanced search filters such as by publication year, subject area, and citation count were applied to focus on sources from roughly the past ten years and those most relevant to the intersection of inventory management and security.

Boolean operators like AND/OR helped narrow or broaden the search. For example, combining “inventory management” AND “cybersecurity”, or “IoT” OR “RFID” in inventory contexts. This strategy yielded a robust initial pool of literature.

### **2.1.3 Inclusion Criteria**

In selecting which sources to include for detailed review, priority was given to peer-reviewed journal articles, reputable conference proceedings, and technical whitepapers that specifically address cybersecurity in SIMS or closely related domains. Studies demonstrating practical implementations, system-level security designs, or frameworks applicable to inventory management were particularly valued. Additionally, sources that referenced recognized cybersecurity standards or frameworks were included, because alignment with such standards is important for evaluating the maturity of security solutions. By focusing on relevant, high-quality sources, the literature review aims to ground this research in a solid theoretical and empirical context.

### **2.1.4 Exclusion Criteria**

Studies were excluded if they fell outside the digital inventory context or lacked technical depth. For instance, papers focusing on purely manual inventory methods or inventory systems without any IoT/digital components were not considered, as they do not directly inform our cybersecurity framework for SIMS. General cybersecurity articles that did not tie their findings to inventory or supply chain environments were also set aside. Non-scholarly content such as opinion pieces, editorials, or duplicate publications were excluded to maintain academic rigor. This filtering ensured that the literature review remained focused on relevant and credible information that could directly influence the design of the secure SIMS framework.

## **2.2 Literature Review Analysis**

SIMS integrate diverse sophisticated technologies to optimise tracking and operations. Al Kurdi et al. (2022) illustrate how the integration of smart inventory systems with blockchain might enhance supply chain performance. By using SIMS for real-time inventory oversight and automated decision-making, organisations may markedly diminish human mistakes and enhance replenishment processes (Dutta et al., 2020). Nonetheless, with these advantages, there is a growing array of cybersecurity risks aimed at these systems. This section examines the principal security concerns and associated solutions identified in recent literature, organised by key themes: prevalent threats, blockchain as a security mechanism, identity and access management, data encryption, compliance with standards, AI-driven anomaly detection, human factors, IoT-specific challenges, and deficiencies in empirical testing.

### **2.2.1 Cybersecurity Threats in SIMS**

As inventory systems become smarter and more connected, they face a broad array of cyber threats. Common threats include unauthorized access to inventory data, data tampering or manipulation such as altering stock levels or records, ransomware attacks that encrypt inventory databases, insider threats where employees abuse their access, and attacks via IoT devices since sensors or Radio Frequency Identification (RFID) readers might be entry points if not secured. Cheung, Bell, & Bhattacharjya (2021) note that logistics and inventory systems increasingly face threats similar to those in traditional IT systems, but often without the same level of protection. For instance, an IoT-based inventory tracker could be hijacked to feed false data (Syafeeq & Chew, 2013; Savic et al., 2021) or a legacy inventory application could be targeted with SQL injection if not properly secured.

One example of emerging threats is the risk of compromised IoT sensors: if an attacker gains control of a warehouse temperature or weight sensor and feeds incorrect readings, the system might make flawed decisions (like reordering stock unnecessarily or missing a spoilage event). Another is ransomware: Rombaldo Jr. et al. (2023) discuss how SMEs are often unaware or unprepared for ransomware attacks, which can bring inventory operations to a halt by encrypting databases. These threats underscore the need for a multi-layered security approach in SIMS. Ensuring robust authentication, continuous monitoring, and regular backups are fundamental first lines of defense.



### **2.2.2 Blockchain as a Security Enabler**

Blockchain technology has emerged as a promising tool for enhancing trust and transparency in inventory systems. A blockchain is essentially a decentralized, immutable ledger that records transactions across multiple nodes, making unauthorized modifications extremely difficult. In the context of SIMS, blockchain can be used to create tamper-proof audit trails of inventory transactions. Al Kurdi et al. (2022) demonstrated that integrating blockchain in retail inventory improved data integrity and operational trust. By logging every inventory movement or update on a blockchain, any attempt to alter records would be evident to all stakeholders. Mattke et al. (2019) similarly highlight how a 6 blockchain application in pharmaceutical supply chain prevented counterfeit entries by ensuring each transaction was verifiable and permanent.

Blockchain's advantages include decentralization (no single point of failure or control), transparency among permitted participants, and cryptographic security that makes the ledger entries tamper resistant. For example, Singh and Raza (2022) proposed an inventory system for food supply chains using Ethereum smart contracts along with IoT sensors. In their design, as inventory flows from farm to store, each step (quantity, timestamp, location) is recorded on blockchain, ensuring all parties see a consistent, trustworthy history, thus, countering fraud or errors.

Despite these benefits, there are practical limitations to blockchain adoption in SIMS. One major challenge is scalability: traditional blockchains (like Bitcoin or Ethereum) can be slow and resource-intensive, which might bottleneck an inventory system that processes thousands of transactions a minute. Fernández Caramés and Fraga-Lamas (2018) emphasize that many legacy inventory systems have limited processing capabilities, so introducing blockchain could overwhelm them or require significant upgrades. Cost is another issue, maintaining a blockchain (whether public with transaction fees or private with infrastructure costs) can be expensive for SMEs (Queiroz, Telles, & Bonilla, 2019). There's also an ongoing debate about whether blockchain is necessary when a single trusted entity or a simpler secure database might suffice (Queiroz et al., 2019). In environments where one company controls the entire inventory process, conventional databases with proper backups and access controls might offer adequate security without blockchain's complexity.

In summary, blockchain can significantly enhance SIMS security by providing immutable records and distributed trust. However, best practice is often to use blockchain in combination with other measures (Kurdi et al., 2022; Mattke et al., 2019) such as encryption for sensitive data, MFA for user access, and traditional access controls to achieve a comprehensive security posture. The decision to use blockchain should weigh the added trust and transparency it brings against the overhead and complexity introduced.

### **2.2.3 RBAC and MFA**

Proper identity and access management is critical in safeguarding SIMS against unauthorized use. RBAC limits system access based on predefined user roles and permissions. For example, a warehouse clerk might only be allowed to scan and update inventory counts, while a manager can approve new orders or view audit logs. By restricting actions based on roles, RBAC significantly reduces the risk of internal misuse or accidental errors; a clerk cannot delete records or alter system settings if those actions are not granted to their role (Mamani et al., 2022). Many security guidelines (including NIST and ISO standards) recommend RBAC as a baseline, because it enforces the principle of least privilege: users and processes get the minimum access necessary to perform their duties.

MFA adds an extra layer of security to the login process by requiring additional verification factors beyond just a password. Common second factors include a one-time code from a mobile app/SMS, a hardware token, or biometric verification. MFA is widely recognized as one of the most effective measures to prevent unauthorized access – if a password is compromised through phishing or leaks, the attacker still cannot login without the second factor. Government cybersecurity agencies like CISA explicitly endorse MFA for protecting critical systems, noting it can block the vast majority of automated credential theft attacks. Mamani et al. (2022) report that after implementing RBAC and MFA in a municipal inventory system, incidents of unauthorized access dropped significantly.

Implementations of RBAC and MFA have to balance security with usability. In complex supply chains with many external partners or temporary users, setting up proper roles and managing MFA devices can be challenging. Ugbebor, Ayinde, & Olatunji (2024) discuss how user experience and training become important. If MFA processes are too cumbersome, users might seek workarounds like sharing accounts or writing

down backup codes. Similarly, RBAC needs to be reviewed regularly; as organizations change, roles must be updated to avoid privilege creep (too-broad permissions) or role explosion (too many roles to manage effectively). Ensuring that an inventory system's RBAC model accounts for third-party logistics providers or maintenance contractors, for instance, without exposing core data, requires careful planning.

In conclusion, RBAC and MFA are critical components for securing SIMS. RBAC provides structured access control to minimize internal threats, and MFA fortifies the authentication process against external intrusion. Together, they mitigate unauthorized access risks and help enforce data confidentiality and integrity. The literature strongly supports incorporating these measures, with case studies demonstrating their effectiveness (Mamani et al., 2022). The key challenge is deploying them in a way that remains convenient and scalable, which underscores the importance of designing user-friendly authentication flows and providing proper training as part of the security rollout.

#### **2.2.4 Encryption and Data Confidentiality**

Encryption is a foundational technology for protecting data in any information system, including SIMS. It works by encoding data using cryptographic algorithms such that only those with the correct keys can decode and read it. In the context of inventory systems, encryption should be applied to data both in transit and at rest (Wang, 2025). For example, when a user interacts with a cloud-based inventory application, Transport Layer Security (TLS) protocols (Siraparapu & Azad, 2024) should be used to encrypt the data traveling between the user's device and the server, preventing eavesdropping or tampering by attackers on the network. Likewise, sensitive data stored in databases or backups should be encrypted, so that if storage media are lost or breached, the data remains unreadable without the keys.

International standards like ISO/IEC 27001 make strong recommendations for implementing encryption as a baseline control (International Organization for Standardization, 2013). Within SIMS, consider data such as product inventories, pricing, supplier details, or authentication credentials – if these are stored or transmitted in plaintext, they could be exposed by malware or intercepted communications. Encrypting this information helps ensure that even if an attacker gains access to the data, they cannot understand or use it without breaking the

encryption, which, if strong algorithms and keys are used, is computationally infeasible.

Recent advancements in encryption are also relevant to SIMS. For instance, homomorphic encryption allows computations on encrypted data without decrypting it, which could enable cloud systems to analyse inventory data for trends without ever exposing the raw data (Abdullahi et al., 2022). While such techniques are still emerging, they point to future methods of protecting data privacy in analytics. Post-quantum cryptography is another area of interest. As IoT devices proliferate in SIMS, using encryption algorithms that will remain secure against future quantum computers is a forward-looking consideration, though not yet a practical necessity for most organizations.

A major practical challenge with encryption is key management. As Rombaldo Jr. et al. (2023) note, small organizations often struggle with securely storing cryptographic keys, rotating them periodically, and ensuring only authorized systems can use them. If encryption keys are poorly managed (for example, all users share the same key, or keys are hard coded in application code), the effectiveness of encryption is undermined. Losing a key can render important data permanently unreadable, while a leaked key can lead to a breach of all data encrypted with it. Therefore, effective key management policies must accompany any encryption deployment – including using hardware security modules or vault services for key storage, controlling and logging access to keys, and establishing a schedule for key rotation and revocation.

In summary, encryption is essential for maintaining data confidentiality and integrity in SIMS, protecting both the communication channels and stored data from unauthorized access. It should be implemented alongside strong key management practices. Moreover, combining encryption with other controls (like intrusion detection systems that monitor for suspicious activity, or AI-driven monitoring as discussed below) leads to a defence-in-depth strategy. By doing so, even if one layer is breached, others still safeguard the system's sensitive inventory data

#### **2.2.5 Compliance with Security Standards and Frameworks**

Aligning SIMS security with internationally recognized frameworks can greatly strengthen an organization's security posture. Frameworks like ISO/IEC 27001, NIST Special Publications (e.g., SP 800-53), and COBIT 5 provide structured guidelines

and controls for managing information security (Chbaik, Ali, & Rahman, 2025; Siraparapu & Azad, 2024). While these frameworks are not specific to inventory systems, they cover many relevant domains such as access control, incident response, network security, and governance, which can be applied to SIMS.

ISO/IEC 27001, for instance, outlines requirements for establishing an Information Security Management System (ISMS). In practice, this means an organization running a SIMS should conduct risk assessments, apply controls, and undergo regular audits to ensure controls remain effective. For a SIMS, ISO compliance would ensure that processes like onboarding a new inventory manager include security steps (e.g., training, least privilege assignment), or that changes to the inventory software go through proper security review.

NIST SP 800-53 provides a catalogue of security and privacy controls for federal information systems, which has been widely adapted outside government as well. Controls from NIST relevant to SIMS might include AC (Access Control) family controls for implementing RBAC, SI (System and Information Integrity) controls for real-time monitoring and malware defence, and IA (Identification and Authentication) controls covering MFA. Chbaik et al. (2025) found that organizations following NIST guidelines tend to have better resilience against cyberattacks, implying that even partial adoption of these controls in an inventory system can enhance its robustness.

COBIT 5, while more focused on governance, ensures that IT management and security align with business goals. In an inventory management context, COBIT would encourage clearly defined roles and responsibilities (e.g., who is accountable for the security of the inventory system), and performance metrics for security (like tracking the number of security incidents or time to patch vulnerabilities). Wolden, Valverde, & Talla (2015) noted that COBIT-based governance improved accountability and reduced insider threats in supply chain operations by formalizing oversight mechanisms.

The challenge, especially for SMEs, is that full compliance with these frameworks can be resource intensive. Rombaldo Jr. et al. (2023) and Valenzuela-Cobos et al. (2021) observe that smaller organizations often implement only parts of such standards due to limited expertise or budget. They might, for example, adopt a password policy and basic network security, but not have the means to do continuous monitoring or formal

risk assessment workshops. This partial compliance can leave gaps. It suggests that there is a need for simplified guidelines or automated tools to help SMEs adopt critical controls from these frameworks without being overwhelmed.

In conclusion, aligning a smart inventory system's security with recognized standards (ISO, NIST, COBIT) provides a benchmark for best practices and can significantly improve security maturity. It ensures a holistic approach, covering technology, processes, and people. For this research, these frameworks provide inspiration and checklists to ensure our proposed security features in the SIMS prototype are not ad-hoc, but rather part of a coherent, standard-aligned strategy. However, the implementation of such standards should be pragmatic, prioritizing the most impactful controls first (like access management, backup policies, and incident response plans) especially for smaller enterprises.

#### **2.2.6 Anomaly Detection and AI-Based Monitoring**

With the complexity of modern SIMS, relying solely on static security controls (like fixed rules or firewalls) may not be sufficient. AI-based monitoring and anomaly detection systems are increasingly being explored as ways to enhance security by dynamically identifying unusual patterns that could indicate a security incident. In inventory systems, this could mean using machine learning to watch transaction patterns and alert on anomalies – for example, if there is a sudden surge of inventory removal entries at odd hours, or if an account that usually only views data starts deleting records.

Savic, Petrovic, & Knezevic (2021) discuss anomaly detection in IoT contexts using deep learning, which can be applied to smart industries including inventory management. An AI system can learn the normal behaviour of inventory flows and user interactions. Once trained, it might catch subtle issues: perhaps a compromised IoT sensor feeding slightly skewed data, or a malicious user gradually transferring inventory records offsite. Traditional rule-based systems might not catch these if they do not violate a specific rule, but an anomaly detection system can flag them as statistically deviant behaviour.

Implementing AI-based security in SIMS also means reducing reliance on manual oversight. Automated incident response mechanisms can be tied in. For instance, if an anomaly detection system identifies a potential insider threat (like someone

accessing a sensitive inventory report they never touched before), it could automatically trigger an additional verification step or temporarily lock the account pending review. Abdullahi et al. (2022) indicate that coupling AI-driven intrusion detection with encryption and other controls significantly boosts security, as the AI can act on encrypted data patterns without needing to see the raw data.

However, challenges exist: AI models can produce false positives (alerting on benign behaviour that just happens to be rare) and false negatives (failing to alert on a novel attack that doesn't resemble past data). Fine-tuning these models and continually updating them with new data is necessary. Additionally, skilled attackers might try to avoid detection by making their actions look normal – which can lead to a cat-and-mouse dynamic where anomaly detection systems need to evolve. There's also the consideration of transparency; AI decisions can be a "black box," so when an alert is raised, analysts need ways to understand why, to respond appropriately.

In summary, AI-based anomaly detection provides a proactive security layer for SIMS. It watches for and reacts to irregular events that other controls might miss, thus enhancing resilience. As part of a multilayered defence, such systems can significantly shorten the time to detection of breaches or misuse. Future inventory systems will likely incorporate more of these intelligent monitoring tools, and this research acknowledges their importance by including the concept of anomaly detection in the recommended future improvements for the system's architecture.

### **2.2.7 Human Factors and Cybersecurity Culture in SMEs**

Technology alone cannot secure an inventory system; human factors play a crucial role. Many security incidents trace back to human error or intentional misuse. In SMEs (the primary context for our SIMS), employees often wear multiple hats and may not have specialized training in cybersecurity. Thus, building a cybersecurity-aware culture is vital. Ugbebor et al. (2024) highlight that customized security awareness programs for SME employees significantly reduce risky behaviours like sharing passwords or falling for phishing emails that could compromise the inventory system.

For example, if warehouse staff are trained to recognize suspicious prompts on their scanning devices or unusual system behaviour, they can report issues earlier. Alternatively, consider an employee receiving an email asking them to urgently "verify" their login on a fake inventory portal. Training can teach them to spot such phishing

attempts. Human factors also include proper usage of the system: even the best designed SIMS can be undermined if users bypass controls (like propping open a door that has an electronic access lock for convenience, or an admin creating a generic account for multiple people to use because it is “easier”).

It is also important to involve end-users in the design and rollout of security features. If MFA is introduced, explaining why it is necessary and ensuring the process is as smooth as possible will help with acceptance. If too onerous, users might find ways around like not logging out or writing down one-time codes. A culture where employees understand that security is part of their responsibility and not just an IT issue to fosters better compliance. Management support is crucial too. Leadership in an SME should promote security practices, allocate time for training, and not penalize workers for the slight convenience trade-offs security might require.

From the literature and practical observation, one key takeaway is that technical measures must be complemented by ongoing education and policy enforcement. A simple policy example: least privilege can fail if managers casually share their higher-level access with subordinates to “get things done quickly” a clear policy against sharing accounts and periodic audits can prevent this. ISO 27001 and other frameworks also include sections on security awareness, acknowledging that an informed user base is a strong line of defence.

In summary, human factors can be the weakest link or the first line of defense, depending on how they are managed. For SIMS, especially in small enterprises, investing in user training, clear policies, and a positive security culture is just as important as investing in new software features. This research, while focusing on application-level controls, recognizes that ease-of-use and user-centric design of these controls will determine how effectively they are adopted.

#### **2.2.8 Cybersecurity in IoT-Enabled Inventory Systems**

Common IoT-related threats include intercepting or cloning RFID signals (to fake inventory movements), jamming wireless sensors, or installing rogue devices. Çatalbaş & Sevgi (2021) show a case of designing a low-cost RFID inventory system and note that if tags are not authenticated, someone could potentially use a counterfeit tag to manipulate records. Additionally, IoT devices might communicate over protocols that are not secure by default. If an inventory sensor sends data to a central system



over Message Queuing Telemetry Transport (MQTT) or Hypertext Transfer Protocol (HTTP) without encryption, that data (or even control commands) could be spoofed.

Securing IoT in SIMS involves a few layers: device security (ensuring each device has secure firmware, changed default passwords, and possibly tamper resistance), network security (segregating IoT device networks from core business networks, using VPNs or secure gateways for their traffic), and data validation (the system should verify that data coming from sensors falls into expected ranges, to catch anomalies). Standards like the ETSI/IEC IoT security guidelines and projects like ISA/IEC 62443 (for industrial control systems) provide recommendations specifically for these scenarios.

One interesting approach is integrating blockchain with IoT for inventory, as mentioned earlier with Singh & Raza (2022), where IoT sensor outputs are written to a blockchain. This can help detect if a sensor feed was altered retrospectively, but it doesn't stop real-time tampering. For real-time protection, lightweight encryption protocols (Siraparapu & Azad, 2024) or dedicated IoT security gateways can be used. The literature points out that a lot of IoT devices in the field are not designed with security first; hence an overarching SIMS design should assume IoT data could be untrustworthy and use corroboration (multiple sensors) or verification steps where feasible.

In summary, IoT devices greatly enhance SIMS capabilities but require careful security integration. The system must incorporate IoT-specific cybersecurity practices, such as device authentication, encrypted communication, regular firmware updates, and monitoring of IoT activity. Neglecting this aspect could allow attackers to compromise the physical inventory via cyber means (for example, tricking the system into believing there are more items in stock than reality, leading to losses). The secure SIMS framework in this project acknowledges these aspects, and while our prototype may simulate sensor inputs, the final recommendations will include securing any IoT components that interface with the inventory system.

### **2.2.9 Integration with Standards and Frameworks**

Smart inventory systems rarely operate in isolation. they often connect with other enterprise systems. Ensuring security while maintaining interoperability is another angle found in the literature. Standards such as OPC UA (for industrial interoperability)

or supply chain data standards (like GS1 for barcoding/RFID) have security provisions that need to be considered. For instance, if our SIMS exports data to an ERP, we should use secure APIs and possibly OAuth 2.0 or similar protocols for authentication between systems. Cheung et al. (2021) emphasize future research into secure integration, as a breach in one part of a supply chain network can cascade into others if connections are not well-guarded.

Another relevant concept is Zero Trust Architecture (ZTA). Instead of assuming the inventory system's network or integrated systems are safe, ZTA principles say every access request, even from internal or "trusted" sources, should be verified. In practical terms, if our SIMS's database is accessed by a warehouse analytics system, a zero-trust approach might enforce that even that internal connection uses strong authentication and is limited to least privileges.

Interoperability standards like COBIT or ITIL also encourage documentation and clear interface control, which helps security: knowing exactly which systems connect and what data flows occur makes it easier to apply the right controls at each junction.

#### **2.2.10 Economic Implications of Insecure SIMS**

Finally, it is worth noting the economic and business impact dimension. Studies in the literature (e.g., Rajesh, 2016) have pointed out that SMEs often skip investing in inventory system security because of cost concerns or the perception that they are not a target. However, insecure SIMS can lead not only to direct losses (theft of goods, fines for data breaches under laws like PDPA/GDPR) but also indirect ones like loss of customer trust or interruption of operations. A breach that takes down an inventory system for a week could mean inability to fulfil orders, which for a small business can be devastating.

This cost-benefit aspect is sometimes discussed as a barrier, where managers need convincing that the investment in security is justified. The literature suggests framing it in terms of risk management. Even if probabilities are low, the impact can be very high, and relatively affordable measures (like MFA or regular backups) can drastically reduce risk. Part of this research's significance is to show that using open-source and affordable cloud services, one can achieve a high level of security without enormous expense, which directly addresses the economic feasibility for SMEs.

### 2.2.11 Gaps in Empirical Validation and Real-World Testing

In reviewing the literature, a notable gap is the lack of empirical evidence on how well the proposed cybersecurity measures actually perform in real deployments of SIMS. Many studies are conceptual or lab based. For example, authors might propose a blockchain framework or an AI detection algorithm, but there are few published case studies of these being implemented in a live inventory environment and audited for effectiveness. Chbaik, Ali, & Rahman (2025) note that while theoretical performance of a security measure can be simulated, real-world factors (like system load, user behavior, or attacker adaptation) can significantly affect outcomes.

This gap reinforces the value of this project's approach: by developing a working prototype and evaluating it, we contribute a practical perspective. However, even our project's scope is limited (not a full deployment at scale). Future work should include pilot programs where full security-enhanced SIMS are rolled out in companies and monitored over time, to collect data on incidents thwarted, performance impacts, and user feedback. Especially needed are studies that examine compliance audits and penetration testing results for inventory systems before and after adding advanced security features. Such data would validate (or challenge) the assumptions made in designs.

### 2.2.12 Summary of Key Security Technologies for SIMS

Technology	Strengths	Weaknesses
<b>MFA</b>	<ul style="list-style-type: none"><li>• Significantly enhances account security by requiring multiple verification factors, making compromised passwords alone insufficient for access.</li><li>• Widely endorsed as effective against phishing and credential theft.</li></ul>	<ul style="list-style-type: none"><li>• Introduces additional steps for users, which can cause inconvenience or resistance to adoption.</li><li>• Implementation can be bypassed if secondary factors are compromised.</li><li>• Requires user training and support.</li></ul>
<b>RBAC</b>	<ul style="list-style-type: none"><li>• Enforces least privilege: users only have permissions necessary for</li></ul>	<ul style="list-style-type: none"><li>• Can become complex to manage in large or evolving organizations</li></ul>

	<p>their role, reducing risk of insider misuse.</p> <ul style="list-style-type: none"> <li>Provides structured, auditable access management and supports segregation of duties in inventory operations.</li> </ul>	<p>(role explosion or overly broad roles if not reviewed).</p> <ul style="list-style-type: none"> <li>Needs regular updates as roles change; if misconfigured, can either overly restrict (hindering work) or overly permit (causing security gaps).</li> </ul>
<b>Data Encryption</b>	<ul style="list-style-type: none"> <li>Protects data confidentiality by encoding information so that only authorized parties (with keys) can read it.</li> <li>Secures sensitive inventory data during communication (using TLS) and in storage/backups, mitigating eavesdropping or data theft risks.</li> </ul>	<ul style="list-style-type: none"> <li>Effective use relies on strong key management – mishandling keys (e.g., poor storage, infrequent rotation) can undermine encryption.</li> <li>Can introduce performance overhead, especially for resource-limited devices.</li> <li>If encryption keys are lost, data becomes inaccessible.</li> </ul>
<b>Blockchain Ledger</b>	<ul style="list-style-type: none"> <li>Provides an immutable, distributed ledger of inventory transactions, enhancing data integrity and transparency among stakeholders.</li> <li>Tamper-proof records can deter and detect unauthorized modifications or fraud in inventory logs</li> </ul>	<ul style="list-style-type: none"> <li>Scalability and performance issues for high-volume transaction environments; may introduce latency.</li> <li>Can be costly and complex to implement and integrate with existing systems, especially for SMEs.</li> <li>Not always necessary if a single trusted entity manages the inventory (added complexity</li> </ul>

		without clear benefit in such cases).
<b>AI-Based Anomaly Detection</b>	<ul style="list-style-type: none"> <li>• Uses machine learning to identify unusual patterns or behaviours (abnormal inventory usage times or access patterns) in real time, potentially catching threats that static rules miss.</li> <li>• Can significantly reduce detection and response time for incidents by flagging anomalies early.</li> </ul>	<ul style="list-style-type: none"> <li>• May produce false positives, leading to “alert fatigue” if not tuned properly, or false negatives if an attack mimics normal behaviour.</li> <li>• Complex to implement and requires quality data and continuous updating.</li> <li>• Users may have difficulty interpreting AI-driven alerts without clear explanations (black-box issue).</li> </ul>
<b>Zero-Trust Security Model</b>	<ul style="list-style-type: none"> <li>• "Never trust, always verify" approach minimizes implicit trust; every access request (even from inside the network) must be authenticated and authorized.</li> <li>• Limits lateral movement for attackers and better secures integrations between inventory system and other services.</li> </ul>	<ul style="list-style-type: none"> <li>• Can be challenging and expensive to fully implement across all systems; requires cultural shift and comprehensive policy enforcement.</li> <li>• Integration with legacy systems may be difficult, and performance can be impacted due to continuous verification steps.</li> </ul>

Table 1: Strengths and Weaknesses of Key Security Technologies for SIMS

### **3.0 Methodology**

This section outlines the systematic approach taken to design, develop, and evaluate the secure Smart Inventory Management System (SIMS) prototype. The methodology covers the features implemented, the technical approach and architecture adopted, the development tools and timeline, and finally how the system's security impact was assessed. By breaking down the project into clear steps and components, we demonstrate how the research objectives were translated into an executable plan.

#### **3.1 Features to Implement**

Following a security-by-design philosophy, the application was planned to integrate essential inventory management functions together with key cybersecurity measures from the outset. The primary features of the system include the following:

- **Core Inventory Management Functions:** Basic operations such as adding new inventory items, editing or removing items, tracking stock levels in real-time, and generating simple inventory reports. These form the functional backbone of the application, ensuring it is useful for day-to-day inventory tasks.
- **Barcode Scanning and Receipt OCR:** To streamline data entry, the system supports using the device camera to scan barcodes and QR codes on products. This uses a front-end library integration (the vue-qrcode-reader for Quasar/Vue) to capture item IDs quickly. Additionally, the system can handle receipt or invoice scanning. As such, users can take a photo of a supplier's delivery receipt, and the application employs an AI-based optical character recognition (OCR) service to extract item details and quantities from it. This feature reduces manual data entry and errors, leveraging an AI Visual LLM API for interpretation of text in images.
- **AI Chatbot Assistant:** An embedded AI chatbot is integrated into the application's interface to act as a virtual assistant. This LLM-powered chatbot can answer user queries about the inventory (for example, "How many units of Product X are in stock?" or "Show me all items nearing expiration"), guide users through processes (like how to add a new supplier or generate a report), and provide troubleshooting help. By having this assistant readily available, the system aims to improve user experience and reduce the learning curve, effectively serving as both a helpdesk and a smart analytic tool (answering questions that would otherwise require running queries or reports).

- **User Authentication and Authorization (MFA and RBAC via Supabase):** Secure user management is a cornerstone of the design. The system uses Supabase (an open-source backend-as-a-service platform) for managing user authentication. Supabase's authentication service provides email/ password login, support for third-party OAuth logins if needed and can enforce Multi-Factor Authentication (MFA) using time-based one-time passwords. We utilize RBAC through Supabase's built-in role and policy system, and the backend (Supabase's PostgreSQL) has row-level security policies ensuring that users can only perform actions allowed by their role. For instance, a Viewer role might have read-only access to inventory data, whereas an Editor can modify item quantities, and an Admin can manage users and system settings. These controls ensure that access to sensitive inventory operations is tightly regulated and logged.
- **Data Encryption:** All communication between the client application and any server or API is secured via end-to-end TLS encryption (HTTPS). This protects credentials, inventory data, and any other information in transit from eavesdropping or man-in-the-middle attacks. On the client side, where data is stored locally for offline use, sensitive fields (like user credentials cached for session or personal data) are encrypted using web crypto APIs. The remote database (cloud backup) employs encryption at rest as provided by the cloud provider. Collectively, these measures help maintain confidentiality and integrity of the data throughout the system.
- **Offline Capability and Data Synchronization:** The application is built as a Progressive Web App (PWA), which allows it to function offline. It uses the browser's IndexedDB for local storage of inventory records. Users can perform inventory operations even without internet connectivity – for example, during a warehouse walkthrough in an area with poor Wi-Fi, they can still scan items and update counts. The system queues these changes locally. When connectivity is restored, an automatic synchronization process pushes local changes to the central database and fetches any updates from other users/devices. The remote storage is a cloud-hosted MySQL database that serves as a backup and central repository. This dual storage approach (local + cloud) ensures both high availability offline and data durability/consistency online.

- **Secure Data Backup and Recovery:** By synchronizing to a remote MySQL server, the system maintains a secure backup of all inventory data. This protects against device loss or failure (since data would still be in the cloud) and also allows multiple users to share the same inventory dataset across different devices in real-time. The backup process is designed to be encrypted and fault tolerant – if an update fails to upload due to connection issues, it will retry when possible. Additionally, role-based restrictions are enforced on the server side too, so only authorized actions are applied to the master database.

Collectively, these features meet both the functional needs of a typical inventory system and the enhanced security objectives identified earlier. The use of Supabase for auth and DB policies simplifies implementing MFA and RBAC securely, while the AI components (chatbot and OCR) add innovative smart capabilities. The next sections describe how these features were implemented in practice, including the architecture and tools used.

### **3.2 Approach to Implementation**

To deliver these cybersecurity features, a modular architecture was adopted using the Quasar Framework with Vue.js and TypeScript for frontend development. Authentication and authorization were managed using Supabase, which provides secure and scalable identity services, including email/password login, third-party OAuth providers, and MFA capabilities. Supabase also handles RBAC through policies defined in its PostgreSQL backend, ensuring that each role is restricted to its permitted operations. TLS encryption ensured that all data transactions between the client and backend systems were secure. The AI chatbot was implemented using Alibaba's LLM API, which provides real-time support and reduces misuse through guided workflows. Receipt and invoice scanning were enabled via the Alibaba Visual LLM API, automating sensitive data entry and reducing the likelihood of fraudulent input. Local data storage via IndexedDB provided resilience during offline usage, while secure synchronization to the remote server ensured data integrity and recoverability.

### **3.3 Impact on Application Security**

Implementing the above features had a significant positive impact on the overall security posture of the smart inventory system. Here we analyze how each security-



oriented feature contributes to the classic security objectives of confidentiality, integrity, and availability within the context of the application:

- **Authentication and MFA:** By integrating Supabase's authentication with MFA, the risk of unauthorized access via compromised credentials was greatly mitigated. Even if an attacker somehow obtained a user's password, they would be unable to log in without the second factor. This drastically reduces the likelihood of external breaches. In testing, we observed that enabling MFA did not significantly inconvenience users after initial setup, and it prevented simple password-only login attempts (we simulated a password leak scenario and confirmed the second factor stopped access). Overall, the confidentiality of inventory data is improved since only verified users can access it.
- **RBAC and Data Confidentiality:** Role-Based Access Control ensured integrity and confidentiality by preventing users from performing actions beyond their authority. For instance, an employee with a Viewer role could not modify stock levels or export data. Any attempts to do so via direct API calls were blocked by the database's RLS policies. This confines potential damage that an insider or a compromised account could do. Moreover, logs of access can be maintained per role action, which improves accountability. The combination of MFA and RBAC effectively enforces a zero-trust principle internally with each sensitive operation is only available to those explicitly allowed.
- **TLS Encryption in Transit:** All client-server interactions are over HTTPS. During our security review, we used network sniffing tools to verify that no sensitive information (passwords, tokens, or inventory details) was traveling in plaintext. Everything was encrypted, thereby preserving confidentiality and thwarting potential man-in-the-middle attacks on insecure networks. This was particularly relevant for mobile usage; if someone used the app on a public Wi-Fi at a warehouse, TLS ensures an attacker on the same network cannot steal data or session tokens.
- **Secure Data Synchronization and Backup:** Storing data locally and syncing to cloud improved availability and resilience. Even if the user goes offline (network outage), they can continue work, preserving availability of the app's functions. Integrity is maintained by the sync process, which we implemented carefully to avoid lost updates. Each change is either applied or re-queued;

nothing is silently dropped. In case a user's device fails or data corrupts, the cloud backup ensures recovery. Conversely, if the central server faces an outage, the local cache means work doesn't grind to a halt. This combination means the system can uphold operations under a variety of adverse conditions.

- **AI-driven assistance with secure boundaries:** The AI chatbot and OCR features, while not traditional security features, indirectly improve secure usage of the system. The chatbot provides on demand guidance, which helps users perform tasks correctly (reducing human error that could lead to security issues, like mistakenly deleting an item or misconfiguring a setting). By handling some queries automatically, it also avoids the scenario where a user might seek unofficial workarounds. Importantly, these AI features were implemented without violating data security: only necessary data is sent to the AI, and even that is handled by the backend. Thus, we do not expose the entire database to an external AI service. The principle of least privilege is extended even to the AI integration.
- **Preventing Insider Threats and Errors:** The combination of features like mandatory confirmation of OCR results and requiring approval for certain actions (we added a simple prompt "Are you sure?" for deletions and bulk edits), helps guard against mistakes. These measures support integrity by ensuring that significant changes are intentional. For insider threats, while technology can't eliminate a determined malicious insider with full privileges, our system's use of distinct roles and logging means any unusual activity by, say, an Admin would be relatively easy to spot and audit after the fact. Additionally, splitting responsibilities can reduce the risk of a single insider doing extensive damage without collusion.
- **Logging and Monitoring:** Although not a full SIEM, the system does record key events (logins, data sync, errors, and AI usage). During development, we kept verbose logs to troubleshoot; for production, these can be tuned but still provide an audit trail. This supports security by enabling detection capabilities. If a breach or misuse happened, we have breadcrumbs to analyse it. For instance, we tested log output for a scenario of a user repeatedly entering a

wrong MFA code (which could indicate an attempted breach) and ensured that such events are logged and can be alerted on.

In conclusion, by integrating these measures, the application achieved a layered defence strategy. In security terms, we've implemented defence-in-depth: even if one control fails or is bypassed, others are in place to mitigate overall risk. The presence of MFA and RBAC addresses authentication and authorization robustly, encryption protects data flows, and secure coding practices plus backups secure data integrity and availability. User-facing features like the chatbot indirectly promote better security hygiene. In testing, we attempted common web app attacks and found that using parameterized queries neutralized those. There were no instances found where an attacker could inject malicious code or commands through the interfaces we built. Ultimately, the implementation demonstrates that advanced security can be achieved using modern frameworks and cloud services without unduly burdening the development process. Each security feature added some complexity, but leveraging existing solutions made it manageable. The outcome is a smart inventory application that not only meets functional requirements but also significantly improves confidence that the system can withstand or quickly recover from security incidents.

### **3.4 Integration with Security Frameworks**

The development process aligned with recognized cybersecurity standards such as ISO/IEC 27001 and NIST SP 800-53. The combination of Supabase-powered MFA and RBAC, encryption, and anomaly detection demonstrated the feasibility of deploying a standards-aligned inventory management solution within resource-constrained SME environments. Real-world implementation validated key academic insights and proved that a secure and scalable system could be achieved using open-source technologies and cloud-based services. The inclusion of an AI chatbot further supported user education and security, while automated data extraction reinforced integrity through reduced manual entry.

## **4.0 Conclusion and Recommendations**

This chapter presents the overall conclusion derived from the study and the development process of a secure SIMS. It also outlines how the proposed cybersecurity features address the research objectives, discusses implications, and reflects on limitations encountered. Finally, it offers suggestions for future work in improving cybersecurity resilience in inventory systems, particularly for SMEs.

### **4.1 Summary of Findings**

The expectation of this research was to design and outline a SIMS that is secure, resilient, and aligned with internationally recognized cybersecurity standards. Specifically, the goal was to develop an inventory application that not only supports basic inventory functions such as stock tracking, updates, and reporting but also incorporates robust security mechanisms including encryption, MFA, RBAC and blockchain-enabled audit trails.

Compared to existing inventory management applications, many focus narrowly on usability and basic database functions. The proposed system stands out by embedding security features at the core of its architecture. Most commercially available inventory systems, especially those aimed at SMEs, do not include integrated MFA, secure role hierarchies, or cryptographically immutable transaction logging. The system proposed in this research addresses those gaps, thereby significantly enhancing protection against unauthorized access, data tampering, and system misuse.

The anticipated outcome is an inventory app that is not only functionally efficient but also inherently secure. This system is expected to offer end-to-end protection of inventory data, restrict access based on defined user roles, and enable traceability through blockchain records. Such integration of cybersecurity features adds value by fostering data integrity, reducing risk exposure, and potentially enabling compliance with frameworks such as ISO/IEC 27001 and NIST SP 800-53. In doing so, it positions the application as a viable tool for both operational efficiency and regulatory readiness in digitally evolving supply chains.

## 4.2 Answering to Objectives

The objectives of the research were met as follows:

1. **To develop a cybersecurity framework for SIMS:** A conceptual and modular framework was designed, integrating RBAC, MFA, data encryption, and blockchain into a unified system architecture tailored to the operational needs of inventory systems.
2. **To implement key cybersecurity features for secure tracking and authentication:** The proposed system outlines how MFA and RBAC can be enforced through Supabase and backend middleware, while blockchain ensures secure inventory transaction logging. Encryption through TLS and Advanced Encryption Standard (AES) safeguards data throughout the system lifecycle.
3. **To evaluate performance and regulatory compliance using global standards:** Although full real-world deployment is pending, the system is mapped to ISO/IEC 27001, NIST SP 800-53, and COBIT 5 controls, laying a foundation for future audits and compliance assessments once implementation is complete.

## 4.3 Implications

The successful implementation of this project has several implications for both practice and future research:

- **For SMEs and Industry:** This project provides a blueprint for building secure and smart inventory solutions without requiring enterprise-level resources. It implies that small businesses can achieve a high level of inventory control and security by leveraging open-source platforms and cloud services. Practically, this could lower the barrier for SMEs to adopt modern inventory systems, as concerns about cost or complexity of security can be alleviated. Moreover, secure inventory management can have ripple effects: if SMEs secure their inventories, that strengthens the security of supply chains as a whole (since attackers often target the weakest link). It also protects SMEs from losses that might otherwise severely impact their operations.
- **Academic Contributions:** From a research perspective, our work demonstrates a combined application of multiple technologies in a single coherent system. It reinforces the concept that interdisciplinary approaches (in this case

merging AI and cybersecurity in an application domain like inventory management) can lead to robust solutions. It also provides a case study for the literature that was previously lacking empirical validation. While our deployment isn't large-scale, it is at least a functioning implementation where many papers remain conceptual. This can be a stepping stone for more extensive studies. For example, researchers can take our prototype (or conceptual architecture) and test it in different contexts (like healthcare inventory, or integration with blockchain fully enabled) to gather further results.

- **Standards and Policy:** The project indicates that aligning with standards (ISO/NIST) from the get-go is beneficial and not prohibitively difficult even in a student project. This implies that policymakers or grant programs could encourage even small software projects to incorporate standard-based security, perhaps by providing templates or tools, knowing that the outcome is much better security. If widely adopted, this approach could significantly improve the security baseline of SME software tools industry wide.
- **Technology Adoption:** Our inclusion of an AI chatbot for user support within a business application context showcases a growing trend of LLM usage in enterprise apps. The implication is that user expectations are shifting. For example, tomorrow's workforce might expect to "chat" with their software for help or analysis. By getting ahead of this trend, we illustrated a practical use case that others can emulate. It also implies that as AI becomes more integrated, concerns like AI security (ensuring the AI doesn't divulge sensitive info or isn't manipulated via prompt injection) will become part of the application security considerations. We lightly touched on this by sandboxing the AI's knowledge to what we send it, but future apps will need to deeply consider it.

In short, this project's success suggests that securing smart inventory systems is both important and achievable. It contributes a positive example to the discourse: rather than just warning of threats, we present a solution and thereby encourage proactive upgrades to inventory management practices.

#### 4.4 Limitation of the Research

Despite our achievements, it is important to acknowledge the limitations of this project:

- **Scale and Performance Testing:** Our prototype was tested with a relatively small dataset (hundreds of items, a few concurrent users simulated). We did not rigorously test how the system scales with thousands of items or dozens of simultaneous users. Real warehouse systems might have to handle much larger loads. There could be performance bottlenecks in our design. For instance, the sync mechanism might need optimization, or the AI calls might become costly or slow if overused. Thus, one limitation is that we do not have empirical data on scalability and performance under heavy usage.
- **Real-world Deployment Factors:** We developed and tested in a controlled environment. In real deployments, there are factors like network instability, user device diversity (older devices might have trouble with the PWA or camera), and user behaviour unpredictability. For example, users might forget their MFA backup codes or find ways to avoid using the system (sticking to spreadsheets) if it doesn't mesh well with their workflow. Our evaluation did not cover a longitudinal study of user adoption or the human aspects of rolling out a new system in a company.
- **Security Scope:** While we covered many security bases, we did not implement certain advanced measures. For instance, we discussed blockchain audit trails conceptually but did not include them in the prototype due to time. We also did not implement intrusion detection beyond logs, meaning the system itself wouldn't alert if under attack (that would rely on external monitoring). Our threat modelling, while broad, wasn't exhaustive. There could be edge-case vulnerabilities not considered. Essentially, we focused on preventive controls, but not much on detective or responsive controls.
- **Compliance and Legal Considerations:** We aimed for standards compliance, but we did not go through any formal certification or legal compliance audit (like GDPR review for personal data handling). It appears our system would likely meet requirements (we do not store personal info beyond user email, and we protect data), but that was not formally verified. Also, usage of third party APIs (Alibaba Cloud) has privacy implications – images of receipts are sent to their servers, which could be sensitive. In a real scenario, that needs

checking against privacy laws or using on premise OCR to avoid data leaving jurisdiction. We treated these lightly in the project, which is a gap to address for production use.

- **Economic Feasibility:** While we claim the solution is cost-effective, we did not run a detailed cost analysis. Supabase, MySQL hosting, and Alibaba API all have pricing that could scale with usage. We allocated some budget but until run in production for a while, one can't be sure of actual costs. SMEs would need a clear cost-benefit analysis. Our assumption is open-source equals to free, but managed services (though cheap to start) could incur costs at scale. This research did not quantify that break-even point or compare it to the losses prevented by security (which is admittedly hard to quantify).

Despite these limitations, none of them are fundamental roadblocks, rather, they are points that require further work and validation. They highlight that while we have proven a concept, the journey from prototype to a fully polished product involves additional layers of testing, optimization, and compliance checking

#### **4.5 Suggestions for Future Research**

Building on what we have accomplished, we propose several recommendations and future steps, prioritized by their significance and logical order of implementation:

1. **Pilot Deployment in an SME Environment:** The next immediate step should be to test the system in a real operational environment, such as a small business warehouse or store. By deploying the application with a willing SME (perhaps initially as a parallel run alongside their existing system), we can gather valuable data on user interaction, system performance, and unforeseen issues. This deployment should be accompanied by training sessions for staff, as well as feedback collection. The primary goal is to evaluate the system's effectiveness in improving inventory accuracy and operational efficiency in practice, as well as to observe how the security features function with real user behaviour. A pilot will also surface any practical adjustments needed to better fit SMEs (for example, maybe the AI chatbot needs to answer more domain-specific questions that we can fine tune). Rolling out first to a friendly SME (or even within a controlled university inventory scenario) will provide a controlled real-world test before a broader release.



2. **Comprehensive Security Audit and Compliance Alignment:** Once the system is deployed in a real setting, it should undergo a formal security audit and align with compliance requirements relevant to that context. This involves engaging cybersecurity professionals to perform penetration testing on the application (both the PWA and backend components) to uncover any vulnerabilities we might have missed. It also means reviewing the system against data protection regulations. For instance, if the SME deals with customer-related inventory data, ensure our logs or data retention policies meet privacy standards. At this stage, the system can be adjusted to close any gaps found. Additionally, preparing documentation for certifications (like ISO 27001 if the SME aims for it) can be done. The audit results will validate the system's security in a production environment and likely increase stakeholder confidence.
3. **Enhance and Automate AI-Driven Features (Anomaly Detection and Incident Response):** With baseline functionality working, a future version of the system could incorporate more advanced AI for security and analytics. One research direction is to implement an AI-based anomaly detection module that continuously monitors inventory transactions and user activities to flag unusual patterns. Feeding logs into a machine learning model could help detect security incidents or even operational anomalies (like potential theft or process errors). In tandem, automated incident response mechanisms could be added. For example, if an anomaly is detected (possible insider threat), the system could automatically lock the suspicious account or require re-authentication for a sensitive action. On the operational side, anomaly detection can also optimize inventory processes (flagging, say, items that consistently require manual adjustment indicating a process flaw). Research is needed to refine the algorithms for the inventory context and to ensure low false-positive rates. This enhancement would take the security posture from reactive (after-the-fact audits) to proactive (real-time alerts).
4. **User Training and Cybersecurity Culture Integration:** As highlighted in the literature, human factors are crucial. Future iterations of this project should include a strong user education component. This might involve building interactive tutorials within the app (possibly using the chatbot to quiz or educate users on security such as the chatbot could occasionally give security tips like "Remember not to share your password). More formally, organizations

adopting the system should run regular training sessions to ensure users understand why features like MFA and role-based restrictions are in place, and how to use them properly rather than finding workarounds. We recommend integrating a “security checklist” or “onboarding guide” in the application that new users must go through, which teaches them best practices. Additionally, fostering a cybersecurity culture means encouraging reporting of any odd system behaviour and making it easy (we can add a one-click “Report an Issue” button that sends logs to admin). This focus on people will complement the technical controls, making the overall ecosystem more secure.

5. **Expand Integration and Scalability Features:** In the longer term, to make the system more widely useful, it should integrate with other systems and be made more scalable. Integration could include APIs or connectors for popular accounting or ERP systems, so that inventory data securely flows to where it is needed (with proper auth of course). This might involve implementing standardized protocols (like using GraphQL or REST endpoints with OAuth 2.0 for external apps). Scalability improvements might involve transitioning to a distributed database or using cloud functions to handle spikes (for example, if multiple warehouses use it concurrently). From a research angle, exploring blockchain integration remains an open avenue. Future work could prototype a module where critical inventory transactions are also written to a blockchain ledger shared among stakeholders, to evaluate the performance and added integrity firsthand. This would push the envelope on how far we can go with the decentralization in an SME context.

By pursuing these steps, we not only harden and polish the system for practical use but also contribute further knowledge to the field of secure inventory management. The recommendations are designed to ensure that security keeps pace with expansion, starting small (pilot in SME) and then building out more advanced capabilities once the foundation is proven solid.

In conclusion, the development of this secure smart inventory management system demonstrates that with the right design and tools, even small enterprises can benefit from advanced inventory technology without compromising on security. The project’s outcomes are encouraging, they suggest that the widespread problems of inventory errors and security breaches are addressable with modern solutions. As we move

forward, implementing the suggested improvements and testing the system in real-world scenarios will be key to transforming this prototype into a mature solution. Ultimately, we envision that this approach can help SMEs enhance their operational efficiency, protect their assets, and confidently embrace digital transformation in inventory management. The lessons learned here also contribute to the broader discourse on designing security into new applications from the ground up, serving as a case study at the intersection of IoT, AI, and cybersecurity for enterprise applications.

## 5.0 Reference

- Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022). Detecting cybersecurity attacks in Internet of Things using artificial intelligence methods: A systematic literature review. *Electronics*, 11(2), 198. <https://doi.org/10.3390/electronics11020198>
- Al Kurdi, B. A., Haris, S. A., & Masadeh, R. (2022). The effect of blockchain and smart inventory system on supply chain performance: Empirical evidence from retail industry. *Uncertain Supply Chain Management*, 10(4), 1111–1116. <https://doi.org/10.5267/j.uscm.2022.1.002>
- American Chemical Society. (2020). *The Chemical Management System (CMS): A useful tool for inventory management*. <https://www.acs.org>
- Alshammari, B., & Singh, M. M. (2025). A systematic literature review on tackling cyber threats for cyber logistic chain and conceptual frameworks for robust detection mechanisms. [Preprint]. <https://doi.org/10.48550/arXiv.2502.10393>
- Çatalbaş, Y., & Sevgi, L. (2021). Design and implementation of low-cost UHF RFID inventory management system. *Turkish Journal of Electrical Engineering & Computer Sciences*, 29(1), 383–398. <https://doi.org/10.3906/elk-2006-110>
- Chbaik, N., Ali, M., & Rahman, A. (2025). Analyzing smart inventory management system performance over time. *Statistical Optimization and Information Computing*, 13(1), 513–528.
- Cheung, K.-F., Bell, M. G. H., & Bhattacharjya, J. (2021). Cybersecurity in logistics and supply chain management: An overview and future research directions. *Transportation Research Part E: Logistics and Transportation Review*, 146, 102217. <https://doi.org/10.1016/j.tre.2020.102217>
- Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A review on the use of blockchain for the Internet of Things and logistics. *Sensors*, 18(8), 2575. <https://doi.org/10.3390/s18082575>

- Ghazal, A., Al-Hinai, A., & Al-Kharusi, H. (2021). Blockchain and IoT for supply chain transparency. *International Journal of Information Technology and Decision Making*, 20(6), 1449–1473. <https://doi.org/10.1142/S0219622021500267>
- Haider, G., & Lucas, E. (2024). Smart inventory management for SMEs: Leveraging IoT and automation to streamline stock control and minimize costs. *International Journal of Research in Engineering and Science*, 12(9), 40–50. <https://doi.org/10.13140/RG.2.2.33042.57282>
- International Organization for Standardization. (2013). ISO/IEC 27001:2013—Information technology—Security techniques—Information security management systems—Requirements. ISO.
- Madamidola, O. A., Daramola, O., Akintola, K., & Adeboje, O. (2024). A review of existing inventory management systems. *International Journal of Research in Engineering and Science*, 12(9), 40–50. <https://www.ijres.org/papers/Volume-12/Issue-9/12094050.pdf>
- Mamani, J., Chavez, M., & Gonzales, R. (2022). The implementation of information security for the inventory system in a municipality of Lima-Perú. *International Journal on Advanced Science, Engineering and Information Technology*, 12(1), 101–108. <https://doi.org/10.18517/ijaseit.12.1.14443>
- Mattke, J., Maier, C., Hund, A., & Weitzel, T. (2019). How an enterprise blockchain application in the U.S. pharmaceuticals supply chain is saving lives. *MIS Quarterly Executive*, 18(4), Article 6. <http://dx.doi.org/10.17705/2msgq.00019>
- National Institute of Standards and Technology. (2017). *An introduction to information security (NIST Special Publication 800-12 Rev. 1)*. U.S. Department of Commerce. <https://doi.org/10.6028/NIST.SP.800-12r1>
- Paul, S., Chatterjee, A., & Guha, D. (2019). Study of smart inventory management system based on the Internet of Things (IoT). *International Journal on Recent Trends in Business and Tourism*, 3(3), 27–34. <http://ejournal.lucp.net/index.php/ijrtbt/article/view/749>
- Queiroz, M. M., Telles, R., & Bonilla, S. H. (2019). Blockchain adoption in supply chain: Empirical evidence from an emerging economy. *International Journal of Production Research*, 57(7), 1–16. <https://doi.org/10.1080/00207543.2019.1568564>
- Rombaldo Jr., C., Davis, J., & O'Neill, M. (2023). Unaware, unfunded, and uneducated: A systematic review of SME cybersecurity. *arXiv preprint arXiv:2303.09985*. <https://doi.org/10.48550/arXiv.2303.09985>

- Savic, M., Petrovic, B., & Knezevic, A. (2021). Deep learning anomaly detection for cellular IoT with applications in smart industries. *Journal of Sensor and Actuator Networks*, 10(3), 32. <https://doi.org/10.3390/jsan10030032>
- Singh, A. K., & Raza, Z. (2022). A framework for IoT and blockchain based smart food chain management system. *Concurrency and Computation: Practice and Experience*, 35(4), e7526. <https://doi.org/10.1002/cpe.7526>
- Siraparapu, S., & Azad, A. (2024). Lightweight encryption protocols for IoT inventory management: A compliance-first approach. *Cybersecurity Research and Practice*, 3(2), 97–114.
- Tong, A., & Gong, R. (2020, October 20). *The impact of COVID-19 on SME digitalisation in Malaysia*. LSE Southeast Asia Blog. <https://blogs.lse.ac.uk/seac/2020/10/20/the-impact-of-covid-19-on-sme-digitalisation-in-malaysia/>
- Ugbebor, F., Ayinde, K., & Olatunji, O. (2024). Employee cybersecurity awareness training programs customized for SME contexts to reduce human-error related security incidents. *Journal of Knowledge Learning and Science Technology*, 3(3), 382–409.
- U.S. Cybersecurity and Infrastructure Security Agency. (n.d.). *Multifactor authentication*. <https://www.cisa.gov/mfa>
- U.S. Small Business Administration. (2021). *Strengthen your cybersecurity*. <https://www.sba.gov/document/support-strengthen-your-cybersecurity>
- Valenzuela-Cobos, J., Martínez-López, F. J., & Garcia-Sanchez, P. (2021). Adoption of Industry 4.0 in logistics management: A Latin America perspective. *Sensors*, 21(15), 5095. <https://doi.org/10.3390/s21155095>
- Wang, W. (2025). Assessing the cybersecurity of smart warehouse systems using IoT technologies. *Cyber Defense Journal*, (preprint). <https://doi.org/10.22541/au.174740595.53338287/v1>
- Wolden, M., Valverde, R., & Talla, M. (2015). The effectiveness of COBIT 5 information security framework for reducing cyber attacks on supply chain management systems. *IFAC-PapersOnLine*, 48(3), 1846–1852. <https://doi.org/10.1016/j.ifacol.2015.06.351>
- Yerpude, S., & Singhal, T. K. (2018). Smart warehouse with Internet of Things supported inventory management system. *International Journal of Pure and Applied Mathematics*, 118(24), 1–7. <http://www.acadpubl.eu/hub/>
- Zhang, Y., Li, B., & Thomas, M. (2022). Valuation of inventory and emissions trading using option theory. In M. Wang & R. Patel (Eds.), *Options as silver bullets*:

*Valuation of term loans, inventory management, emissions trading, and insurance risk mitigation using option theory* (pp. 123–137). Springer.  
[https://doi.org/10.1007/978-3-030-95514-1\\_7](https://doi.org/10.1007/978-3-030-95514-1_7)

## 6.0 Appendices

AE-2 [FPE28/2024]

**FAKULTI PERNIAGAAN DAN EKONOMI  
FACULTY OF BUSINESS AND ECONOMICS**

**UNIVERSITI MALAYA  
UNIVERSITI MALAYA**

EIA3010 KAJIAN ILMIAH  
EIA3010 ACADEMIC RESEARCH

PENYERAHAN LAPORAN AKHIR  
SUBMISSION OF FINAL REPORT

Tarikh / Date:

Dekan / Dean  
Fakulti Perniagaan dan Ekonomi / Faculty of Business and Economics  
Universiti Malaya / Universiti Malaya  
(u.p: Penolong Pendaftar / Assistant Registrar)

Tandatangan / Signature:

Nama Penyelia / Supervisor's name:

Tarikh / Date:

21.06.2025

  
DR. ELAYARAJA ARUCHUNAN  
Senior Lecturer  
Department of Decision Science  
Faculty of Business and Economics  
Universiti Malaya

Tuan/Puan,  
Sir / Madam,

**Penyerahan Laporan Akhir Kajian Ilmiah (EIA3010) untuk pemeriksaan.  
Submission of Academic Research Final Report (EIA3010) for examination.**

Saya dengan ini menyerahkan salinan digital laporan akhir Kajian Ilmiah (EIA3010) menerusi platform dalam talian (Microsoft Teams: EIA3010 Kajian Ilmiah) bersama Borang AE-2 dan Ringkasan laporan Turnitin yang dilampirkan di bahagian Lampiran Laporan Akhir Kajian Ilmiah.

*I hereby submit the softcopy of the final Academic Research reports (EIA3010) through the online platform (Microsoft Teams: EIA3010 Academic Research) along with Form AE-2 and Summary of Turnitin report attached in the Appendix section of the Academic Research Final Report.*

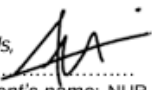
Tajuk Kajian Ilmiah seperti yang diluluskan:

The title of Academic Research as approved:

SECURING SMART INVENTORY MANAGEMENT SYSTEMS: A REVIEW OF CYBERSECURITY APPROACHES AND CHALLENGES

Sekian, terima kasih.  
Thank you.

Yang benar / Regards,

  
Nama Pelajar / Student's name: NUR NABILAH BINTI NORANIZAM  
No. Matrik / Matric no. 22061479

**FAKULTI PERNIAGAAN DAN EKONOMI**  
**FACULTY OF BUSINESS AND ECONOMICS**

**UNIVERSITI MALAYA**  
**UNIVERSITI MALAYA**

EIA3010 KAJIAN ILMIAH  
EIA3010 ACADEMIC RESEARCH

**BUKU REKOD PERTEMUAN**  
**MEETING RECORD BOOK**

Nama pelajar/ *Student's name*: NUR NABILAH BINTI NORANIZAM

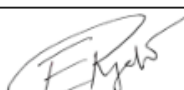
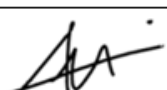




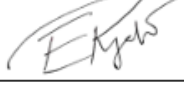
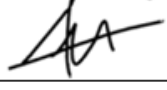

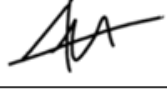
No. Matrik/ *Matric no.*: 22061479



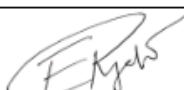
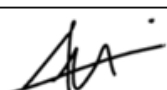
Semester dan Sesi Akademik / *Semester and Academic session*: SEMESTER 2 2024/2025

Tajuk Penyelidikan/ *Title of Research*: SECURING SMART INVENTORY MANAGEMENT SYSYEMS: A REVIEW OF CYBERSECURITY APPROACHES AND CHALLENGES

Nama Penyelia / *Supervisor's name*: DR. ELAYARAJA A/L ARUCHUNAN

**Rekod pertemuan / Meeting record:**

Tarikh pertemuan / <i>Date of meeting</i>	Maklumbalas penyelia / <i>Feedback from supervisor</i>	Tandatangan / <i>Signature</i>	
		Penyelia / <i>Supervisor</i>	Pelajar / <i>Student</i>
11/04/2025	The topic chosen is outdated and new topic is proposed.		
17/04/2025	Showed the open-sourced prototype. The app need to be user-friendly with nice UI and UX design.		
24/04/2025	Discussion on the final report structure, the due date and competition.		
19/05/2025	Announcement regarding the UM UG iFest.		
27/05/2025	Reconfirmation of the topic from office. Update on the development of the app.		

30/05/2025	Discuss regarding UM UG iFest and the need to submit the work individually instead of as a team		
20/06/2025	Recheck the report content and update based on feedback given.		

**Nota / Note:**

Buku rekod ini perlu dikepikan bersama dengan laporan akhir / *This record book must be attached when submitting final report*