



Securing the Digital Warehouse Strengthening Data Protection in Technology-Driven Warehouse Operations

Mohamed Najib Salleh^{1*}, Fadhilah Mohd Zahari²

^{1, 2} School of Technology Management & Logistics, Universiti Utara Malaysia, Malaysia

CORRESPONDING AUTHOR

Mohamed Najib Salleh
Email: najib@uum.edu.my
ORCID: 0000-0000-0000-0000

ARTICLE HISTORY

Received	Revised	Accepted	Published
30 June 2026	4 August 2026	27 August 2026	30 September 2026

ABSTRACT

Digital warehouses increasingly depend on warehouse management systems, Internet of Things devices, cloud platforms, automated handling technologies, artificial intelligence, and interconnected data services. This expansion of digital capability improves visibility and coordination but also enlarges the attack surface through which data manipulation, unauthorised access, service disruption, insider misuse, and compromised connected devices can affect warehouse operations. This conceptual article examines data protection as an operational capability within technology-driven warehousing. It integrates recent research on smart warehousing, cyber-physical risk, IoT security, warehouse management systems, automation, blockchain, and digital resilience to explain how security weaknesses can move from information systems into physical fulfilment processes. Five areas receive particular attention: data integrity and access control, IoT and endpoint exposure, WMS and cloud vulnerabilities, human and insider risk, and cyber resilience across interconnected warehouse ecosystems. The analysis argues that effective protection requires more than isolated cybersecurity tools. Secure architecture, identity governance, data classification, network segmentation, continuous monitoring, recovery capability, supplier assurance, and workforce security practices must operate as a coordinated warehouse governance system. The resulting perspective positions data protection as a foundation for trustworthy automation, reliable inventory information, operational continuity, and resilient digital supply chains.

Keywords: Warehousing, Cybersecurity, Protection, Resilience, Digitalisation

HOW TO CITE

Author1, A. A., & Author2, B. B. (20XX). Title of the article.
International Journal of Business and Management Advancement,
X(X), xx–xx. <https://doi.org/10.xxxx/ijbma.xxxxx>

COPYRIGHT & OPEN ACCESS

Copyright © 2026 The Author(s).
Published by Global Academia Network. This open access article is
licensed under the Creative Commons Attribution (CC BY 4.0)
licence: <https://creativecommons.org/licenses/by/4.0/legalcode>

1. INTRODUCTION

Warehouses have moved from relatively contained storage environments into digitally coordinated operating systems in which inventory records, mobile devices, sensors, automated equipment, cloud services, and external supply chain platforms exchange data continuously. This shift has improved visibility and speed, yet it has also changed the meaning of warehouse risk because a corrupted transaction, compromised identity, unavailable network, or manipulated device can now influence physical fulfilment within seconds. Research on intelligent warehousing describes interconnection and automation as defining characteristics of the smart warehouse (Tubis & Rohman, 2023). Recent studies of highly automated facilities further identify cyberattacks, technology failures, network outages, and human-machine vulnerabilities as material sources of operational disruption (Kembro & Norrman, 2025). Data protection must therefore be treated as part of warehouse operating reliability rather than as a background information technology function. Boysen et al., (2019) demonstrate that increasing warehouse automation changes the operational structure through which digital technologies interact with physical fulfilment activities. The warehouse consequently depends on the confidentiality, integrity, availability, and traceability of information that determines where stock is located, which order is released, what equipment is authorised to move, and whether a transaction is legitimate. Securing the digital warehouse therefore requires a direct connection between cybersecurity controls and the operational consequences of compromised data.

Technology-driven warehouse operations create a particularly demanding security environment because cyber and physical processes are tightly coupled. Warehouse management systems coordinate receiving, put-away, replenishment, picking, packing, and dispatch, while RFID, handheld terminals, IoT sensors, automated storage systems, robots, and cloud applications extend that coordination across numerous endpoints. Each connection can improve process visibility but can also become an entry point for unauthorised access, false data, malware, or service disruption. IoT-based warehouse research demonstrates the growing dependence on connected sensing, while threat-modelling research in digital logistics shows that mobile and distributed IoT devices introduce communication-security concerns that differ from conventional office systems (Jarašūnienė et al., 2023; Junejo et al., 2023). The security objective is therefore broader than preventing disclosure of confidential information, particularly because logistics digitalisation expands the cyberattack surface across interconnected operational systems (Cheung et al., 2021). Warehouse protection must preserve trustworthy inventory states, transaction authenticity, device behaviour, user privileges, and continuity of execution under both malicious attack and technology failure. A useful security model must recognise that warehouse data are operational assets whose compromise can produce immediate financial, service, safety, and supply chain consequences (Junejo et al., 2023).

Current scholarship increasingly recognises that digital warehouse performance depends on the quality of the information architecture supporting automation. Studies of smart warehouse operations emphasise information interconnection, equipment automation, and process integration, while research on warehouse management systems links digital coordination with resilience and competitiveness. These benefits depend on data that are accurate, timely, authorised, and available when operational decisions are executed. Sari and Butun provide direct evidence that contemporary WMS environments face data manipulation, insider threats, fraudulent activity, and accountability weaknesses, and they position immutable logging, IoT tracking, and anomaly detection as complementary security mechanisms (Sari & Butun, 2026; Yusof et al., 2025). The implication is

that warehouse cybersecurity cannot be reduced to perimeter defence. Protection must extend across identities, applications, databases, interfaces, devices, networks, logs, and recovery arrangements, with controls proportionate to the operational importance of each asset. This broader view connects data protection with the reliability of the warehouse process itself and provides a stronger basis for evaluating security investment.

Despite rapid warehouse digitalisation, security maturity does not necessarily develop at the same pace as technological adoption. Organisations often introduce automation, analytics, cloud connectivity, or IoT devices to solve performance problems, then address security after systems have already become operationally embedded. Legacy interfaces, shared credentials, weak device management, inconsistent access rules, and limited recovery testing can remain hidden while normal operations continue. Research on Industry 4.0 warehousing shows broad technological expansion, whereas studies of cloud and IoT security repeatedly identify access control, data protection, interface exposure, and service availability as persistent concerns (Perotti et al., 2024; Ali et al., 2015). This creates a conceptual tension: the same connectivity that produces real-time visibility and automation also increases dependence on digital trust. Efficiency gains may therefore coexist with a larger attack surface and more severe cascading consequences when a critical system is compromised. The unresolved challenge is to explain how warehouses can preserve the benefits of digital integration while systematically controlling the vulnerabilities created by that integration.

This article examines how data protection can be strengthened across technology-driven warehouse operations and why security should be embedded within warehouse management rather than treated as a separate technical concern. The analysis adopts an integrated operational-security perspective that connects warehouse information flows with cybersecurity principles, IoT exposure, WMS and cloud dependence, human behaviour, and resilience. It first establishes the digital foundations that make warehouse data strategically important, then identifies five contemporary protection challenges and interprets the mechanisms through which those challenges affect operational performance. Recent warehouse-specific security research is combined with established work on smart warehousing, digital supply chains, cloud security, automation, and information technology capability to avoid treating cybersecurity in isolation (Sari & Butun, 2026; Büyüközkan & Göçer, 2018). The intended contribution is a structured explanation of how secure architecture, identity governance, trustworthy data, controlled connectivity, monitoring, recovery, and workforce capability can function as mutually reinforcing elements of digital warehouse protection. This perspective positions security as an enabling condition for dependable automation, accurate inventory control, resilient fulfilment, and sustainable digital transformation.

2.0 LITERATURE REVIEW

Digital warehouse security begins with understanding what must be protected and why it matters operationally. Modern warehouses depend on critical data, connected endpoints, warehouse management systems, cloud services, automated equipment, artificial intelligence, and external digital relationships. These elements create value through integration, yet the same integration creates dependencies that can transmit error or malicious activity across processes. The five foundations below establish how data protection relates to information integrity, IoT security, application and cloud security, cyber-physical exposure, and digital resilience. Together they frame

security as an operational architecture that preserves trustworthy warehouse decisions rather than as a collection of isolated technical controls.

2.1 Strategic Digital Warehouse Data Security Supporting Operational Capability

Warehouse data have become operationally critical because digital systems increasingly determine the location, status, ownership, priority, and movement of inventory. A single warehouse transaction can influence replenishment, order allocation, labour tasks, transport planning, customer promises, and financial reconciliation. The value of protection therefore lies not only in keeping information confidential but also in preserving its integrity, availability, provenance, and authorised use throughout the transaction lifecycle. The wider performance effect remains dependent on implementation quality because, as Yusof et al., (2025) observes, technology adoption alone does not guarantee sustained organisational value. Smart warehouse research consistently emphasises information interconnection as a foundation for integrated operations, while strategic warehouse studies link information capability with wider supply chain performance (Zhen & Li, 2022; Abdullah et al., 2020). This means that corrupted master data, altered stock quantities, falsified timestamps, or unauthorised order changes can propagate beyond the warehouse and create errors that appear operationally legitimate. Security controls must consequently be aligned with data criticality and process impact rather than applied uniformly to every information asset. Treating warehouse data as a governed operational asset establishes the first foundation for a security architecture that protects both information and fulfilment performance. Smart warehouse architecture increasingly depends on integrated cyber-physical systems capable of coordinating inventory information, technology, and operational control (Fernando et al., 2024).

Evidence from Sari and Butun (2026) reinforces this interpretation. The strategic importance of warehouse data becomes more pronounced as artificial intelligence and automated decision systems are introduced. Algorithms used for slotting, replenishment, picking priorities, anomaly detection, and resource allocation depend on historical and real-time data that may originate from multiple devices and applications. If those inputs are manipulated or incomplete, automation can execute incorrect decisions at a scale and speed that manual controls may not detect immediately. Research on AI-enabled warehouse transformation and IoT-assisted machine learning illustrates how digital intelligence increasingly depends on continuous operational data, while security-centric WMS research identifies manipulation and reconciliation weaknesses as direct threats to system integrity (Yusof et al., 2025; Wang, 2023). Data protection must therefore include validation, lineage, access accountability, and monitoring for unusual changes, not merely encryption or backup. The organisation needs to know who changed critical data, which system generated it, whether the change was authorised, and how rapidly an incorrect state can be isolated. Reliable digital warehouse intelligence begins with protected data whose origin, meaning, and integrity can be trusted throughout automated decision processes.

2.2 Connected Endpoint Security Across Digital Warehouse Infrastructure

Connected devices expand warehouse visibility by capturing inventory movement, environmental conditions, equipment status, and user activity close to the physical process. RFID readers, handheld scanners, sensors, gateways, cameras, mobile terminals, and embedded controllers reduce manual information gaps, yet they also distribute computing and communication functions across a large and diverse endpoint population. Many devices have long service lives, constrained hardware,

vendor-specific firmware, or limited patching arrangements. Junejo et al. show that IoT-enabled digital logistics requires security analysis that reflects mobile and potentially uncontrolled deployment conditions, while warehouse IoT research demonstrates how extensively sensor data can support modern operational management (Junejo et al., 2023; Jarašūnienė et al., 2023). The security challenge is therefore architectural because heterogeneous IoT environments require coordinated authentication, access control, privacy, and trust mechanisms across connected devices (Sicari et al., 2015). An attacker does not need to compromise the central WMS if a weak endpoint can provide credentials, falsify sensor data, expose an interface, or become a foothold for lateral movement. Device identity, secure configuration, firmware governance, network segmentation, and authenticated communication become essential warehouse controls. Endpoint security is consequently inseparable from the trustworthiness of the operational data generated at the warehouse floor.

Kembro and Norrman (2025) provides an important basis for understanding this warehouse security concern. IoT security in warehouses also requires attention to the relationship between device availability and physical workflow continuity. A sensor or scanner may appear low risk when assessed only by the sensitivity of the data it stores, yet its failure can stop receiving confirmation, location verification, automated routing, or inventory updates. Security classification should therefore consider operational dependency as well as conventional information sensitivity. Studies of highly automated warehouses demonstrate that technology failures and network outages can become significant operational disruptions, and smart warehouse reviews show that connected technologies increasingly span multiple warehouse processes (Kembro & Norrman, 2025; Tubis & Rohman, 2023). This changes prioritisation. Devices supporting critical execution paths require stronger redundancy, monitoring, replacement capability, and fallback procedures than peripheral devices, even when both process similar data. Security teams and warehouse managers must jointly identify which endpoints can interrupt throughput or corrupt inventory states. A risk-based endpoint model connects cyber protection with process criticality and prevents organisations from underestimating seemingly simple devices that occupy decisive positions in digital warehouse workflows.

2.3 Warehouse Management Systems Cloud Platforms Application Security

Sari and Butun (2026) identifies a comparable operational concern in digitally connected environments. The warehouse management system is a high-value security target because it translates commercial demand into executable warehouse activity. User accounts, inventory records, task queues, interface messages, configuration rules, and transaction histories converge within the WMS or its surrounding application ecosystem. Cloud delivery and software integration can improve scalability and accessibility, but they also introduce dependencies on identity services, APIs, remote administration, vendor controls, and shared infrastructure. Cloud security research has long identified confidentiality, integrity, availability, virtualisation, and service-model risks, while recent warehouse-specific work shows that WMS abuse can involve insider manipulation, fraudulent transactions, and weak accountability (Subashini & Kavitha, 2011; Ali et al., 2015). Application security must therefore combine secure authentication, least-privilege authorisation, change control, interface protection, logging, vulnerability management, and tested recovery. The strongest control is not necessarily the most restrictive one; it is the control that prevents unauthorised actions without

obstructing legitimate warehouse execution. Protecting the WMS means protecting the decision layer through which digital information becomes physical movement.

Zhang et al., (2010) provides an important basis for understanding this warehouse security concern. Cloud-connected warehouse applications also shift part of security responsibility beyond the physical boundary of the facility. Service providers may operate infrastructure, identity components, databases, monitoring tools, or integration services that warehouse personnel cannot directly inspect. This does not remove organisational accountability for operational risk; instead, it requires clearer understanding of shared responsibilities and stronger assurance over external dependencies. Foundational cloud research explains how service abstraction changes control and dependency, while digital supply chain research shows that interconnected platforms increasingly support cross-organisational information exchange (Zhang et al., 2010; Hashizume et al., 2013). Warehouse governance must therefore examine service-level commitments, incident notification, data location, backup, portability, privileged vendor access, interface security, and exit arrangements. A secure cloud configuration can still produce operational weakness if recovery assumptions are untested or if a critical integration has no alternative path. This relationship is also documented by Büyüközkan and Göçer (2018). Cloud security becomes meaningful to warehouse management when contractual, technical, and operational controls are integrated around the continuity and integrity of fulfilment processes.

2.4 Automation Artificial Intelligence Cyber Physical Security Exposure

Automation changes warehouse cybersecurity because digital instructions can directly influence physical equipment and material flow. Automated storage and retrieval systems, conveyors, mobile robots, sorters, and intelligent picking technologies operate through software, sensors, control logic, and networked communication. A malicious or erroneous command can therefore produce congestion, misrouting, unavailable equipment, incorrect inventory movement, or unsafe interactions. Azadeh et al. document the increasing sophistication of robotised warehouse systems, while recent analysis of highly automated warehouses identifies technology sabotage, cyberattacks, failures, outages, and human-machine vulnerabilities as distinct disruption categories (Azadeh et al., 2019; Kembro & Norrman, 2025). Cyber-physical protection must account for safe states, command authentication, separation of control networks, anomaly detection, maintenance access, and the ability to continue or stop operations safely when digital trust is lost. Predictive cyber-risk analytics also becomes increasingly important as Industry 4.0 supply chains rely on interconnected IIoT environments (Radanliev et al., 2020). Conventional office-security assumptions are insufficient because availability and deterministic control can be as important as confidentiality. The more deeply automation is integrated into warehouse execution, the more cybersecurity becomes a condition of physical operational control. Distributed cyber-physical warehouse architectures further show that operational components increasingly depend on interconnected computational agents, communication, and data exchange (Piardi et al., 2023).

Artificial intelligence introduces a different but related layer of exposure because decision quality depends on models, data, and feedback loops that may not be transparent to warehouse users. AI can improve forecasting, task allocation, anomaly detection, and resource optimisation, yet manipulated training data, misleading inputs, poorly governed model changes, or excessive trust in automated recommendations can create new forms of operational error. Security therefore extends into model

governance and human oversight. Warehouse research increasingly associates AI with digital automation and smart inventory management, while Sari and Butun propose AI-driven anomaly detection as one element of a broader security-centric WMS architecture (Yusof et al., 2025; Sari & Butun, 2026). The important distinction is between using AI as a security tool and securing AI-enabled operations themselves. Organisations need controlled model deployment, validated data sources, explainable escalation rules, and clear authority for overriding automated decisions when operational evidence conflicts with system output. Trustworthy automation depends on a security model that protects both the infrastructure executing decisions and the information logic through which those decisions are produced.

2.5 Digital Resilience Security Governance Across Warehouse Operations

Digital resilience provides the organisational bridge between preventive security and continued warehouse performance when prevention fails. No technology-driven warehouse can eliminate every vulnerability, particularly when it depends on complex software, external services, connected devices, human users, and changing threat conditions. The relevant capability is the ability to detect abnormal conditions, contain their spread, preserve critical operations, recover trustworthy data, and restore services within acceptable operational limits. Research on warehouse management systems links digital capability with supply chain resilience, while broader logistics studies emphasise adaptive strategies for maintaining performance under disruption (Yusof et al., 2025). Resilience therefore requires more than backup copies. Recovery priorities must reflect warehouse process dependencies, including which systems are required for receiving, inventory verification, order release, picking, dispatch, and customer communication. Manual fallback procedures also need current data and trained personnel if they are to function during a digital outage. Evidence from Kembro and Norrman (2025) reinforces this interpretation. Security governance becomes strategically valuable when it converts technical recovery objectives into warehouse-specific continuity capabilities.

Perotti et al., (2024) identifies a comparable operational concern in digitally connected environments. Effective security governance also determines whether protection remains aligned with technological change after implementation. Digital warehouses evolve continuously as new devices, interfaces, automation modules, analytics tools, and external partners are added. A security design that was adequate at deployment can become obsolete when system relationships change or temporary exceptions become permanent operating practices. Research on digital transformation indicates that technological value depends on complementary organisational capabilities, and studies of smart technologies in warehousing similarly show that integration choices shape operational outcomes (Yusof, 2025). Governance must therefore establish ownership for cyber risk, periodic asset discovery, access review, vulnerability remediation, change assessment, supplier assurance, incident learning, and measurable security performance. These activities should be embedded within warehouse management routines rather than activated only during audits or after incidents. A digitally mature warehouse is not one with the most technology, but one that can expand technological capability without allowing security responsibility, data integrity, or operational resilience to deteriorate.

3.0 DIGITAL WAREHOUSE VULNERABILITIES RESHAPING OPERATIONAL SECURITY RISK

The digital warehouse faces vulnerabilities that arise from the way technologies are connected, governed, and used in practice. Fragmented data protection can weaken accountability; unmanaged IoT devices can enlarge the attack surface; cloud and third-party dependencies can concentrate disruption; human workarounds can bypass carefully designed controls; and weak recovery arrangements can extend the operational impact of an incident. These challenges are closely connected to the digital foundations established earlier. They demonstrate that cybersecurity risk is created not only by external attackers but also by architectural complexity, unclear ownership, operational pressure, and inadequate preparation for failure. The following analysis examines these vulnerabilities through their warehouse consequences.

3.1 Fragmented Data Protection Increasing Privileged Access Risk

Sari and Butun (2026) provides an important basis for understanding this warehouse security concern. Fragmented data protection emerges when warehouse information is distributed across WMS databases, spreadsheets, handheld devices, automation controllers, cloud applications, and partner interfaces without a consistent control model. Different systems may apply different authentication rules, retention practices, permissions, and audit capabilities. Privileged users can accumulate broad access because operational teams prioritise speed and availability, while old accounts or shared credentials remain active to avoid interrupting work. Security-centric WMS research identifies insider manipulation and accountability gaps as direct risks, while cloud security studies show that access control remains fundamental when services and data are distributed (Sari & Butun, 2026; Ali et al., 2015). The operational consequence is that unauthorised changes may appear as valid warehouse transactions and can be difficult to distinguish from normal activity. Excessive privilege also increases the impact of stolen credentials because one identity may reach several critical processes. Fragmentation therefore weakens both prevention and investigation, making identity governance and data ownership central warehouse management concerns.

The wider strategic problem is that fragmented access control undermines trust in the digital record on which automated fulfilment depends. If managers cannot establish who approved an inventory adjustment, changed a location rule, altered an order priority, or exported sensitive data, the warehouse loses accountability even when the system remains technically available. This can affect reconciliation, customer disputes, regulatory obligations, and confidence between supply chain partners. Warehouse digital capability, as Yusof et al., (2026) explains, depends on aligning technology use with operational priorities. Research on digital supply chains emphasises the value of integrated information, while warehouse strategy studies connect information quality and coordination with performance (Büyüközkan & Göçer, 2018; Abdullah et al., 2020). Current responses often focus on passwords or periodic user reviews, but these controls are insufficient when privileges are inherited through roles, interfaces, service accounts, and third-party administration. The risk increases during organisational change, peak-season staffing, system migration, or emergency access. A stronger response must connect identity lifecycle management with warehouse process authority so that digital permissions accurately reflect operational responsibility.

3.2 Expanding IoT Attack Surfaces Across Unmanaged Warehouse Endpoints

This relationship is also documented by Alaba et al., (2017). The rapid growth of connected warehouse devices creates an attack surface that is difficult to manage through conventional endpoint practices. Sensors, RFID infrastructure, scanners, gateways, cameras, mobile terminals, and embedded controllers may be procured from different vendors and managed by different teams. Some devices cannot support modern security agents, receive patches slowly, or use default services that remain enabled after installation. Threat modelling for IoT-enabled logistics demonstrates the importance of communication security in distributed devices, while warehouse IoT studies show the operational breadth of connected sensing (Junejo et al., 2023; Jarašūnienė et al., 2023). An unmanaged endpoint can become a route into wider networks, a source of falsified operational data, or a persistent blind spot that is absent from standard asset inventories. The risk is intensified when devices are physically accessible or when maintenance interfaces are exposed for convenience. The central challenge is maintaining security visibility across a device population designed primarily for operational function rather than enterprise cybersecurity.

Endpoint proliferation also creates a governance problem because responsibility can be divided among warehouse operations, engineering, information technology, vendors, and facilities teams. When ownership is unclear, patching, credential rotation, certificate renewal, logging, and replacement decisions may be delayed until a failure occurs. Operational pressure can reinforce this weakness because managers are understandably reluctant to interrupt equipment that is meeting throughput targets. Studies of highly automated warehouses show that technology vulnerabilities can produce cascading disruption, while reviews of Industry 4.0 warehousing illustrate the increasing density of interconnected technologies (Kembro & Norrman, 2025; Tubis & Rohman, 2023). The limitation of many current responses is that they treat each device as an isolated technical asset rather than part of a process dependency chain. A scanner used at dispatch and a noncritical environmental sensor should not receive identical resilience priorities simply because both are IoT devices. Risk classification must combine cyber exposure with the operational consequence of device compromise or unavailability.

3.3 Cloud Dependencies Increasing Warehouse Application Security Vulnerabilities

Modern warehouses increasingly depend on external software services, cloud infrastructure, integration platforms, and vendor support arrangements that extend the security boundary beyond direct organisational control. A WMS may rely on remote identity services, hosted databases, API gateways, transport platforms, e-commerce systems, or managed automation software. A failure or compromise in one dependency can affect warehouse execution even when local equipment remains functional. Cloud security research identifies shared responsibility and service dependence as persistent challenges, while WMS research shows how central digital platforms have become to resilience and competitiveness (Subashini & Kavitha, 2011; Zhang et al., 2010). The difficulty is that warehouse managers may understand operational processes in detail without having equivalent visibility into upstream digital dependencies. Contractual uptime targets can also create false confidence if recovery procedures, data portability, or integration restoration have never been tested. Third-party risk therefore becomes warehouse risk whenever an external digital service participates in a critical fulfilment path.

The strategic consequence of service dependence is concentration risk: a highly integrated platform can improve coordination during normal operations while becoming a single point of disruption

during an incident. This tension is especially important in multi-site networks where the same cloud service, identity provider, or software release supports several facilities. A common vulnerability can therefore affect multiple warehouses simultaneously and remove the possibility of shifting work to an unaffected site. Warehouse digital capability, as Yusof et al., (2025) explains, depends on aligning technology use with operational priorities. Digital supply chain research stresses interconnection and visibility, while recent warehouse disruption research shows how technology failures and outages can cascade through operations (Büyüközkan & Göçer, 2018; Kembro & Norrman, 2025). Traditional business continuity plans may underestimate this pattern if they assume that disruption remains local. Effective protection requires mapping common digital dependencies across sites, understanding vendor recovery capabilities, and identifying which warehouse functions can operate independently when central services are unavailable. Resilience must therefore be designed at network level rather than assessed facility by facility (Kembro & Norrman, 2025).

3.4 Human Behaviour Increasing Insider Exposure Security Workarounds

Human behaviour remains a major source of warehouse security exposure because operational work frequently rewards speed, continuity, and rapid problem solving. Employees may share devices, reuse credentials, bypass approval steps, connect unauthorised equipment, or create manual data files when systems are slow or unavailable. These actions are often intended to keep work moving rather than to cause harm, yet they weaken traceability and create opportunities for deliberate misuse. The wider performance effect remains dependent on implementation quality because, as Yusof et al., (2025) observes, technology adoption alone does not guarantee sustained organisational value. Sari and Butun identify insider threats and product abuse as relevant WMS risks, while warehouse digitalisation studies show that human roles continue to interact closely with increasingly automated systems (Sari & Butun, 2026; Perotti et al., 2024). Security controls that ignore workflow realities can unintentionally encourage workarounds. If authentication is too slow for high-frequency tasks or access requests take longer than operational deadlines, users will search for alternative routes. The challenge is therefore behavioural and organisational as well as technical: secure practice must be designed so that the correct action is also practical within warehouse operating conditions.

Insider exposure becomes more complex when warehouses use temporary labour, contractors, maintenance specialists, system integrators, and vendor technicians. These groups may require short-term access to devices, applications, restricted areas, or administrative functions, but their access lifecycle can be poorly synchronised with operational schedules. Credentials may remain active after assignments end, while emergency vendor accounts can escape normal monitoring. Information technology capability research indicates that organisational processes and technology resources must be aligned, and digital transformation studies similarly emphasise capability development rather than technology acquisition alone (Yusof et al., 2020). A narrow awareness-training response does not address these structural weaknesses. Organisations need role design, time-limited access, segregation of duties, privileged-session monitoring, rapid offboarding, and clear accountability for third-party activity. Human-centred security becomes effective when governance anticipates how people actually enter, use, support, and leave the digital warehouse environment. The resulting capability strengthens trust in digital records while reducing the likelihood that a local technology weakness develops into a wider supply chain disruption.

3.5 Weak Cyber Recovery Limiting Digital Warehouse Resilience

Many warehouses invest more heavily in preventing cyber incidents than in proving that critical operations can recover from them. Backups may exist without recent restoration tests, incident plans may be written without warehouse-specific process priorities, and manual procedures may depend on data that becomes unavailable during the same outage. Recovery objectives can therefore look adequate on paper while failing to reflect the pace of fulfilment operations. Highly automated warehouse research identifies outages and technology failures as major disruption categories, and resilience-oriented WMS research shows that digital capability increasingly shapes continuity (Kembro & Norrman, 2025; Yusof et al., 2025). The weakness becomes visible when teams must decide which systems to restore first, how to verify inventory after recovery, whether automated equipment can reconnect safely, and how orders processed during downtime will be reconciled. These decisions require preparation before an incident. Cyber resilience must therefore be measured through recoverability of warehouse processes, not merely through the existence of technical backup infrastructure (Kembro & Norrman, 2025).

Limited resilience also creates strategic exposure because prolonged warehouse disruption can propagate into transport schedules, customer service, production continuity, and supplier coordination. The cost of a cyber incident is consequently not confined to system restoration. Lost throughput, inventory uncertainty, missed dispatch windows, emergency labour, expedited transport, and reputational damage can exceed direct technology costs. This is especially significant where distribution networks operate with limited buffers. Strategic warehouse and digital supply chain studies emphasise the warehouse role in wider network performance, while recent security-centric WMS research connects system integrity with financial accountability and operational efficiency (Abdullah et al., 2020; Büyüközkan & Göçer, 2018). Current continuity approaches often separate cyber incident response from supply chain contingency planning, creating gaps between technical recovery and business recovery. A warehouse may regain system access yet remain unable to trust inventory records or resume automated execution safely. Sari and Butun (2026) identifies a comparable operational concern in digitally connected environments. Resilience requires coordinated recovery of data, systems, physical flow, and supply chain commitments.

4.0 SECURITY MECHANISMS STRENGTHENING DIGITAL WAREHOUSE OPERATIONAL PERFORMANCE

The significance of warehouse cybersecurity becomes clearer when protection is interpreted through the mechanisms that preserve operational trust. Identity governance establishes who is authorised to act; data integrity determines whether digital records can be trusted; segmentation limits the spread of compromised devices; dependency transparency clarifies where external services can affect operations; human-centred design reduces insecure workarounds; and resilience enables recovery when preventive controls fail. These mechanisms explain why identical technologies can produce different security outcomes across warehouses. Effective protection depends on how controls interact with warehouse processes, decision rights, system architecture, and recovery capability rather than on technology deployment alone.

4.1 Identity Governance Protecting Data Integrity Across Warehouse Operations

Identity governance explains why access control must be connected to operational authority rather than managed as a generic user-administration task. In a digital warehouse, permission to adjust inventory, release orders, change locations, modify interfaces, or administer automation carries different operational consequences. Role design should therefore follow process responsibility, while privileged actions require stronger authentication, approval, and traceability. Research evidence supports this interpretation (Sari & Butun, 2026; Yusof et al., 2026). The mechanism is important because warehouse security decisions become more effective when technical controls are tied to the specific process consequence they are intended to prevent. Rather than adding isolated safeguards, the organisation creates a coherent control environment in which information, access, technology, and operational authority reinforce one another. This reduces ambiguity during normal operations and provides clearer decision rights when abnormal activity is detected. Evidence from Abdullah et al., (2020) reinforces this interpretation. The resulting capability strengthens trust in digital records while reducing the likelihood that a local technology weakness develops into a wider supply chain disruption (2020).

Data integrity complements identity governance because authorised access does not guarantee that information remains correct. Validation rules, immutable or tamper-evident logs, segregation of duties, reconciliation controls, and anomaly detection create multiple opportunities to detect inappropriate change before it propagates into physical execution. This interpretation is consistent with relevant warehouse and digital security research (Sari & Butun, 2026). The strategic implication is that protection must remain usable, observable, and recoverable under real operating conditions (Roy et al., 2025). Security maturity is demonstrated not by the number of controls deployed but by the organisation's ability to maintain trustworthy warehouse decisions when technology, people, or external services behave unexpectedly. The resulting capability strengthens trust in digital records while reducing the likelihood that a local technology weakness develops into a wider supply chain disruption.

4.2 Zero Trust Segmentation Securing Connected Warehouse Devices

Junejo et al., (2023) provides an important basis for understanding this warehouse security concern. The logic of zero trust is particularly relevant to warehouses because device location inside a facility should not automatically imply that the device or its traffic is trustworthy. Connected scanners, sensors, gateways, controllers, and maintenance laptops should be authenticated according to identity and function, with communication limited to the services genuinely required for operation. Research evidence supports this interpretation (Junejo et al., 2023; Alaba et al., 2017). The mechanism is important because warehouse security decisions become more effective when technical controls are tied to the specific process consequence they are intended to prevent. Rather than adding isolated safeguards, the organisation creates a coherent control environment in which information, access, technology, and operational authority reinforce one another. This reduces ambiguity during normal operations and provides clearer decision rights when abnormal activity is detected. The resulting capability strengthens trust in digital records while reducing the likelihood that a local technology weakness develops into a wider supply chain disruption.

Segmentation also changes incident containment. When device networks are flat, a compromised endpoint can provide a path toward applications or control systems unrelated to its legitimate role.

Functional network zones, authenticated gateways, monitored east-west traffic, and restricted maintenance paths reduce this lateral movement without requiring every device to support sophisticated security software. This interpretation is consistent with relevant warehouse and digital security research (Kembro & Norrman, 2025; Tubis & Rohman, 2023). The strategic implication is that protection must remain usable, observable, and recoverable under real operating conditions. Security maturity is demonstrated not by the number of controls deployed but by the organisation's ability to maintain trustworthy warehouse decisions when technology, people, or external services behave unexpectedly. This relationship is also documented by Ali et al., (2015). The resulting capability strengthens trust in digital records while reducing the likelihood that a local technology weakness develops into a wider supply chain disruption.

4.3 Shared Responsibility Strengthening Warehouse Ecosystem Dependency Transparency

Evidence from Subashini and Kavitha (2011) reinforces this interpretation. Cloud and third-party risk can be interpreted through the principle of dependency transparency. Warehouse leaders cannot govern what they do not know they depend on. A complete service map should connect warehouse processes to applications, interfaces, identity providers, data stores, networks, vendors, and recovery arrangements so that operational consequences are visible before disruption occurs. Research evidence supports this interpretation (Zhang et al., 2010; Hashizume et al., 2013). The mechanism is important because warehouse security decisions become more effective when technical controls are tied to the specific process consequence they are intended to prevent. Rather than adding isolated safeguards, the organisation creates a coherent control environment in which information, access, technology, and operational authority reinforce one another. This reduces ambiguity during normal operations and provides clearer decision rights when abnormal activity is detected. The resulting capability strengthens trust in digital records while reducing the likelihood that a local technology weakness develops into a wider supply chain disruption.

Shared responsibility becomes practical only when responsibilities are translated into testable controls. The organisation may rely on a provider for infrastructure availability while remaining responsible for user privileges, configuration, data classification, integration security, and operational fallback. Contracts cannot substitute for internal understanding of these boundaries. This interpretation is consistent with relevant warehouse and digital security research (Ali et al., 2015; Büyüközkan & Göçer, 2018). The strategic implication is that protection must remain usable, observable, and recoverable under real operating conditions. Security maturity is demonstrated not by the number of controls deployed but by the organisation's ability to maintain trustworthy warehouse decisions when technology, people, or external services behave unexpectedly. The resulting capability strengthens trust in digital records while reducing the likelihood that a local technology weakness develops into a wider supply chain disruption.

4.4 Human Centred Security Supporting Operationally Usable Warehouse Controls

Human-centred security explains why warehouse controls must fit the tempo and physical conditions of operational work. Employees wearing gloves, moving between zones, sharing workstations across shifts, or responding to exceptions experience security controls differently from office users. Controls that create excessive delay can produce predictable workarounds and reduce the quality of audit trails. Research evidence supports this interpretation (Perotti et al., 2024; Yusof, 2022). The mechanism is important because warehouse security decisions become more effective when

technical controls are tied to the specific process consequence they are intended to prevent. Rather than adding isolated safeguards, the organisation creates a coherent control environment in which information, access, technology, and operational authority reinforce one another. This reduces ambiguity during normal operations and provides clearer decision rights when abnormal activity is detected. The resulting capability strengthens trust in digital records while reducing the likelihood that a local technology weakness develops into a wider supply chain disruption.

The same principle applies to insider-risk management. Effective control does not begin by treating employees as threats; it begins by reducing unnecessary privilege, separating sensitive duties, monitoring exceptional activity, and making legitimate access easy to obtain and easy to remove. This design reduces opportunity for both accidental and deliberate misuse. The wider performance effect remains dependent on implementation quality because, as Yusof et al., (2020) observes, technology adoption alone does not guarantee sustained organisational value. This interpretation is consistent with relevant warehouse and digital security research (Sari & Butun, 2026; Yusof, 2025). The strategic implication is that protection must remain usable, observable, and recoverable under real operating conditions. Security maturity is demonstrated not by the number of controls deployed but by the organisation's ability to maintain trustworthy warehouse decisions when technology, people, or external services behave unexpectedly. The resulting capability strengthens trust in digital records while reducing the likelihood that a local technology weakness develops into a wider supply chain disruption (Sari & Butun, 2026).

4.5 Cyber Resilience Strengthening Digital Warehouse Performance Capability

Cyber resilience is best understood as the ability to preserve or restore acceptable warehouse performance when digital trust is disrupted. This shifts attention from abstract recovery-time metrics toward concrete questions: which orders can still be processed, how inventory will be verified, which equipment can operate safely, and what data are required to reconcile work completed during degraded operation. Research evidence supports this interpretation (Kembro & Norrman, 2025; Yusof et al., 2025). The mechanism is important because warehouse security decisions become more effective when technical controls are tied to the specific process consequence they are intended to prevent. Rather than adding isolated safeguards, the organisation creates a coherent control environment in which information, access, technology, and operational authority reinforce one another. This reduces ambiguity during normal operations and provides clearer decision rights when abnormal activity is detected. Evidence from Abdullah et al., (2020) reinforces this interpretation. The resulting capability strengthens trust in digital records while reducing the likelihood that a local technology weakness develops into a wider supply chain disruption.

A resilience perspective also encourages learning after disruption. Incident review should not stop at the technical root cause; it should examine why the incident affected throughput, which dependencies amplified the impact, where manual procedures failed, and what information was unavailable to decision makers. These lessons can then reshape architecture and operating procedures. This interpretation is consistent with relevant warehouse and digital security research (Yusof et al., 2025; Büyüközkan & Göçer, 2018). The strategic implication is that protection must remain usable, observable, and recoverable under real operating conditions. Security maturity is demonstrated not by the number of controls deployed but by the organisation's ability to maintain trustworthy warehouse decisions when technology, people, or external services behave

unexpectedly. The resulting capability strengthens trust in digital records while reducing the likelihood that a local technology weakness develops into a wider supply chain disruption.

5.0 STRATEGIC CAPABILITY PATHWAYS SECURING RESILIENT DIGITAL WAREHOUSE OPERATIONS

Strengthening the digital warehouse requires coordinated action that addresses the specific vulnerabilities identified in the preceding analysis. The pathways below align security architecture with warehouse execution by combining identity and data governance, segmented IoT protection, WMS and supplier assurance, human-centred security practices, and operational cyber recovery. Each pathway is designed to be implementable rather than aspirational. The emphasis is on ownership, control mechanisms, measurable outcomes, and continuous improvement so that security can evolve with automation and digital connectivity. Collectively, these pathways establish data protection as a capability that supports reliable information, safe automation, business continuity, and resilient supply chain performance.

5.1 Risk Based Identity Access Data Governance Practices

A stronger protection model should begin with a warehouse-specific inventory of critical data and privileged actions. Organisations should classify inventory, order, customer, supplier, device, and configuration data according to operational impact, then map who can view, change, approve, export, or administer each category. Access should be role-based, least-privileged, time-bounded where appropriate, and reviewed when employees or contractors change responsibilities. The proposed pathway is supported by relevant research (Sari & Butun, 2026; Ali et al., 2015). Implementation should assign accountable owners, measurable control objectives, and review intervals so that protection remains aligned with changing warehouse technology and process priorities. The expected outcome is not simply lower cyber risk, but greater confidence that digital information can be used safely to coordinate inventory and fulfilment. The resulting capability strengthens trust in digital records while reducing the likelihood that a local technology weakness develops into a wider supply chain disruption.

Sari and Butun (2026) provides an important basis for understanding this warehouse security concern. Implementation should combine multifactor authentication for sensitive functions, privileged-access management, segregation of duties, automated joiner-mover-leaver processes, and tamper-evident logging for high-impact transactions. Data quality controls should flag unusual adjustments, duplicate events, unexpected master-data changes, and transactions outside normal operational patterns. Research provides further support for this capability-building approach (Sari & Butun, 2026; Roy et al., 2025). Operational resilience can also be strengthened when, as Yusof et al., (2025) indicates, digital systems are integrated with appropriate organisational capability. Performance should be reviewed through both security and operational indicators so that management can see whether controls reduce exposure without creating unacceptable delay. Over time, this approach converts security from a reactive technical function into a repeatable warehouse capability that supports reliable digital growth. The resulting capability strengthens trust in digital records while reducing the likelihood that a local technology weakness develops into a wider supply chain disruption.

5.2 Segmented Architecture Securing Iot Automation Warehouse Systems

Warehouses should create a controlled architecture for connected devices rather than allowing each technology project to introduce its own security pattern. Every device should have an identified owner, known firmware state, approved communication path, unique identity where technically possible, and defined replacement or isolation procedure. New devices should enter production only after configuration and vulnerability checks. The proposed pathway is supported by relevant research (Junejo et al., 2023; Jarašūnienė et al., 2023). Implementation should assign accountable owners, measurable control objectives, and review intervals so that protection remains aligned with changing warehouse technology and process priorities. The expected outcome is not simply lower cyber risk, but greater confidence that digital information can be used safely to coordinate inventory and fulfilment. Alaba et al., (2017) identifies a comparable operational concern in digitally connected environments. The resulting capability strengthens trust in digital records while reducing the likelihood that a local technology weakness develops into a wider supply chain disruption (2017).

Network design should separate user, IoT, automation, guest, and administrative traffic according to operational need. Gateways should authenticate communications between zones, remote maintenance should use controlled access paths, and abnormal device behaviour should be monitored centrally. Where legacy devices cannot support modern controls, compensating measures should restrict their reach and increase monitoring. Research provides further support for this capability-building approach (Kembro & Norrman, 2025; Azadeh et al., 2019). Performance should be reviewed through both security and operational indicators so that management can see whether controls reduce exposure without creating unacceptable delay. Over time, this approach converts security from a reactive technical function into a repeatable warehouse capability that supports reliable digital growth. The resulting capability strengthens trust in digital records while reducing the likelihood that a local technology weakness develops into a wider supply chain disruption.

5.3 Warehouse Cloud Supplier Security Assurance Capability Development

Subashini and Kavitha (2011) provides an important basis for understanding this warehouse security concern. WMS and cloud protection should be governed through a shared-responsibility model that clearly identifies which controls belong to the organisation, software provider, cloud provider, integrator, and automation vendor. Security requirements should be incorporated into procurement, architecture review, service-level agreements, change management, and renewal decisions rather than assessed only after deployment. The proposed pathway is supported by relevant research (Subashini & Kavitha, 2011; Hashizume et al., 2013). Implementation should assign accountable owners, measurable control objectives, and review intervals so that protection remains aligned with changing warehouse technology and process priorities. The expected outcome is not simply lower cyber risk, but greater confidence that digital information can be used safely to coordinate inventory and fulfilment. The resulting capability strengthens trust in digital records while reducing the likelihood that a local technology weakness develops into a wider supply chain disruption.

Supplier assurance should include evidence of vulnerability management, incident notification, privileged-access control, backup and recovery capability, data portability, and secure software development. Critical interfaces should be authenticated and monitored, while warehouse teams should understand how a provider outage or compromised integration would affect specific operational processes. Research provides further support for this capability-building approach (Ali

et al., 2015; Yusof et al., 2025). Performance should be reviewed through both security and operational indicators so that management can see whether controls reduce exposure without creating unacceptable delay. Over time, this approach converts security from a reactive technical function into a repeatable warehouse capability that supports reliable digital growth. Evidence from Büyüközkan and Göçer (2018) reinforces this interpretation. The resulting capability strengthens trust in digital records while reducing the likelihood that a local technology weakness develops into a wider supply chain disruption.

5.4 Human Behaviour Security Practices Strengthening Warehouse Operations

Security awareness should be redesigned around warehouse decisions rather than delivered as generic annual training. Employees need practical guidance on shared devices, suspicious login prompts, unauthorised USB or network connections, inventory adjustments, lost scanners, vendor access, phishing, and the correct response when digital instructions conflict with physical observations. Supervisors should reinforce these behaviours during routine operational management. Warehouse digital capability, as Yusof (2025) explains, depends on aligning technology use with operational priorities. The proposed pathway is supported by relevant research (Yusof, 2022; Perotti et al., 2024). Implementation should assign accountable owners, measurable control objectives, and review intervals so that protection remains aligned with changing warehouse technology and process priorities. The expected outcome is not simply lower cyber risk, but greater confidence that digital information can be used safely to coordinate inventory and fulfilment. The resulting capability strengthens trust in digital records while reducing the likelihood that a local technology weakness develops into a wider supply chain disruption.

Control design should also reduce incentives for workarounds. Authentication methods should be fast enough for high-frequency tasks, temporary access should be obtainable through controlled processes, and exception procedures should preserve traceability during peak periods or system degradation. Security teams should observe actual workflows before imposing controls that affect productivity. Research provides further support for this capability-building approach (Sari & Butun, 2026; Yusof et al., 2020). Performance should be reviewed through both security and operational indicators so that management can see whether controls reduce exposure without creating unacceptable delay. Over time, this approach converts security from a reactive technical function into a repeatable warehouse capability that supports reliable digital growth. The resulting capability strengthens trust in digital records while reducing the likelihood that a local technology weakness develops into a wider supply chain disruption.

5.5 Cyber Recovery Capability Supporting Continuous Security Improvement

Digital warehouses should maintain recovery plans that are organised around operational processes rather than technology components alone. Recovery priorities should identify the minimum systems, data, devices, people, and external services required to receive goods, confirm inventory, release orders, pick safely, dispatch shipments, and reconcile transactions after service restoration. The proposed pathway is supported by relevant research (Kembro & Norrman, 2025; Yusof et al., 2025). Implementation should assign accountable owners, measurable control objectives, and review intervals so that protection remains aligned with changing warehouse technology and process priorities. The expected outcome is not simply lower cyber risk, but greater confidence that digital information can be used safely to coordinate inventory and fulfilment. The resulting capability

strengthens trust in digital records while reducing the likelihood that a local technology weakness develops into a wider supply chain disruption.

Exercises should test realistic scenarios such as ransomware affecting the WMS, loss of cloud connectivity, compromised administrator credentials, corrupted inventory data, or unavailable automation controllers. Results should be measured through operational outcomes, including time to restore trusted inventory status, throughput under degraded conditions, backlog recovery, and successful reconciliation. Research provides further support for this capability-building approach (Yusof et al., 2025). Operational resilience can also be strengthened when, as Yusof et al., (2025) indicates, digital systems are integrated with appropriate organisational capability. Performance should be reviewed through both security and operational indicators so that management can see whether controls reduce exposure without creating unacceptable delay. Over time, this approach converts security from a reactive technical function into a repeatable warehouse capability that supports reliable digital growth. The resulting capability strengthens trust in digital records while reducing the likelihood that a local technology weakness develops into a wider supply chain disruption (2025).

6.0 CONCLUSION

Protecting the digital warehouse requires a broader understanding of security than the traditional separation between information technology and warehouse operations allows. Inventory accuracy, order execution, equipment coordination, traceability, and service continuity increasingly depend on digital information moving across WMS platforms, cloud services, IoT devices, automation systems, and external supply chain interfaces. The resulting environment creates substantial opportunities for faster and more intelligent operations, but it also means that compromised data or unavailable technology can produce immediate physical and commercial consequences. Data protection is therefore an operating requirement. Its purpose is to preserve the trustworthiness of the information through which warehouse work is authorised, coordinated, recorded, and recovered.

The analysis identifies five closely connected capabilities that determine the security of technology-driven warehouse operations. Identity and data governance protect high-impact transactions and establish accountability. Segmented IoT architecture limits exposure created by expanding device populations. WMS, cloud, and supplier assurance make external dependencies visible and governable. Human-centred controls reduce the gap between formal security requirements and actual warehouse work. Cyber recovery ensures that the organisation can restore trustworthy data and operational flow when preventive measures are insufficient. Their combined value is greater than isolated technical controls because each capability addresses a different pathway through which digital weakness can become warehouse disruption. Security maturity consequently depends on integration across architecture, governance, people, process, and recovery.

The strategic significance of this perspective is that cybersecurity investment can be evaluated according to its contribution to reliable warehouse performance rather than treated only as a technical or compliance cost. Future empirical research can test how specific combinations of access governance, device segmentation, supplier assurance, security behaviour, and recovery maturity influence inventory accuracy, throughput stability, incident impact, and supply chain resilience across different levels of automation. Particular attention is needed in multi-site and highly

automated networks where common digital dependencies can transmit disruption across facilities. As warehouses continue to adopt artificial intelligence, robotics, cloud platforms, and pervasive sensing, the ability to protect data and maintain trusted digital control will increasingly determine whether technological sophistication produces resilience or fragility. Securing the digital warehouse ultimately means ensuring that every layer of technology strengthens, rather than compromises, the reliability of warehouse operations.

DECLARATIONS

1. Acknowledgement

The authors sincerely appreciate the academic support and scholarly environment provided by Universiti Utara Malaysia in supporting the development of this article.

2. Conflict of Interest

The authors confirm that this article was prepared without any financial, personal, or professional interests that could have influenced its content or interpretation.

3. Author Contribution Statement

Mohamed Najib Salleh: Developed the research concept, reviewed the literature on digital warehouse security, constructed the main arguments, and prepared the initial manuscript.

Fadhilah Mohd Zahari: Examined cybersecurity and data protection perspectives, strengthened the discussion on digital resilience, and contributed to manuscript review and final editing.

Both authors reviewed and approved the final manuscript.

4. Ethics Statement

The study followed accepted principles of academic integrity and responsible research practice. As the article is conceptual and draws exclusively on published scholarly sources, no human participation or primary data collection was involved. Ethical approval and informed consent were therefore not applicable.

REFERENCES

- Abdullah, F. I., Yusof, M. S., & Abu Seman, S. (2020). Strategic warehouse management and supply chain performance in a changing business environment. *The Asian Journal of Professional & Business Studies*, 1(2), 73–89. <https://doi.org/10.61688/ajpbs.v1i2.155>
- Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications*, 88, 10–28. <https://doi.org/10.1016/j.jnca.2017.04.002>
- Ali, I., & Phan, H. M. (2022). Industry 4.0 technologies and sustainable warehousing: A systematic literature review and future research agenda. *The International Journal of Logistics Management*, 33(2), 644–662. <https://doi.org/10.1108/IJLM-05-2021-0277>
- Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences*, 305, 357–383. <https://doi.org/10.1016/j.ins.2015.01.025>
- Azadeh, K., De Koster, R., & Roy, D. (2019). Robotized and automated warehouse systems: Review and recent developments. *Transportation Science*, 53(4), 917–945. <https://doi.org/10.1287/trsc.2018.0873>

- Boysen, N., De Koster, R., & Weidinger, F. (2019). Warehousing in the e-commerce era: A survey. *European Journal of Operational Research*, 277(2), 396–411. <https://doi.org/10.1016/j.ejor.2018.08.023>
- Büyükközkın, G., & Göçer, F. (2018). Digital supply chain: Literature review and a proposed framework for future research. *Computers in Industry*, 97, 157–177. <https://doi.org/10.1016/j.compind.2018.02.010>
- 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>
- Fernando, Y., Suhaini, A., Tseng, M.-L., Abideen, A. Z., & Shaharudin, M. S. (2024). A smart warehouse framework, architecture and system aspects under Industry 4.0: A bibliometric networks visualisation and analysis. *International Journal of Logistics Research and Applications*, 27(12), 2688–2711. <https://doi.org/10.1080/13675567.2023.2215179>
- Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, 4, 5. <https://doi.org/10.1186/1869-0238-4-5>
- Jarašūnienė, A., Čižiūnienė, K., & Čereška, A. (2023). Research on impact of IoT on warehouse management. *Sensors*, 23(4), 2213. <https://doi.org/10.3390/s23042213>
- Junejo, A. K., Breza, M., & McCann, J. A. (2023). Threat modeling for communication security of IoT-enabled digital logistics. *Sensors*, 23(23), 9500. <https://doi.org/10.3390/s23239500>
- Kembro, J. H., & Norrman, A. (2025). Managing technology-related disruptions and vulnerabilities in highly automated warehouse systems: An integrative review and research agenda. *International Journal of Production Research*. <https://doi.org/10.1080/00207543.2025.2552281>
- Perotti, S., Cannava, L., Ries, J. M., & Grosse, E. H. (2024). Reviewing and conceptualising the role of 4.0 technologies for sustainable warehousing. *International Journal of Production Research*, 63(6), 2305–2337. <https://doi.org/10.1080/00207543.2024.2396015>
- Piardi, L., Costa, P., Oliveira, A., & Leitão, P. (2023). MAS-based distributed cyber-physical system in smart warehouse. *IFAC-PapersOnLine*, 56(2), 6376–6381. <https://doi.org/10.1016/j.ifacol.2023.10.826>
- Radanliev, P., De Roure, D., Page, K., Nurse, J. R. C., Montalvo, R. M., Santos, O., Maddox, L., & Burnap, P. (2020). Cyber risk at the edge: Current and future trends on cyber risk analytics and artificial intelligence in the Industrial Internet of Things and Industry 4.0 supply chains. *Cybersecurity*, 3, 13. <https://doi.org/10.1186/s42400-020-00052-8>
- Roy, S., Bisht, A., Das, A. K., & Shetty, S. (2025). Age of information-based optimal scheduling with energy cost trade-off for smart warehouse: A deep reinforcement learning-based approach. *IEEE Access*, 13, 163982–163998. <https://doi.org/10.1109/ACCESS.2025.3609200>
- Sari, A., & Butun, I. (2026). A security-centric warehouse management framework for mitigating product abuse and cybersecurity risks. *Computers*, 15(6), 348. <https://doi.org/10.3390/computers15060348>

- Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, 146–164. <https://doi.org/10.1016/j.comnet.2014.11.008>
- Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34(1), 1–11. <https://doi.org/10.1016/j.jnca.2010.07.006>
- Tubis, A. A., & Rohman, J. (2023). Intelligent warehouse in Industry 4.0: Systematic literature review. *Sensors*, 23(8), 4105. <https://doi.org/10.3390/s23084105>
- Wang, Y. (2023). IoT-assisted machine learning model for engineering project warehouse management. *Journal of Computational Methods in Sciences and Engineering*, 23(2). <https://doi.org/10.3233/JCM-226630>
- Yusof, M. S. (2022). Strengthening warehouse operations through integrated safety management practices. *The Asian Journal of Professional & Business Studies*, 1(2), 56–72. <https://doi.org/10.61688/ajpbs.v1i2.150>
- Yusof, M. S. (2025). Technology adoption in small and medium enterprises and its impact on business growth, innovation, and digital sustainability. *International Journal of Advanced Research in Economics and Finance*, 7(3), 84–100. <https://doi.org/10.55057/ijaref.2025.7.3.7>
- Yusof, M. S., Abdul Razak, N., Syed A Rahman, S. N. M., & Salleh, M. N. (2025). Innovative strategies for overcoming challenges in modern logistics and achieving sustainable growth. *International Journal of Business and Technology Management*, 7(2), 220–234. <https://doi.org/10.55057/ijbtm.2025.7.2.20>
- Yusof, M. S., Ahmad Zaini, A. F., Zainal Abidin, Z., & Wahid, A. (2025). The transformation of modern warehouse operations through artificial intelligence, digital automation, and smart inventory management. *International Journal of Business and Technology Management*, 7(2), 365–379. <https://doi.org/10.55057/ijbtm.2025.7.2.32>
- Yusof, M. S., Fauzi, N., Jamaludin, A., Seman, S. A., Salleh, M. N., & Tasrip, N. E. (2025). Technological advancements in vending machines transforming consumer behavior market trends and the future of automated retail. *Journal of Posthumanism*, 5(6), 139–149. <https://doi.org/10.63332/joph.v5i6.1968>
- Yusof, M. S., Fauzi, N., Mat Yusop, Z., Mohamad Yunus, M. H. S., & Wahid, A. (2025). Advanced approaches to enhancing picking and packing efficiency through smart automation and optimization. *International Journal of Business and Technology Management*, 7(2), 14–25. <https://doi.org/10.55057/ijbtm.2025.7.2.3>
- Yusof, M. S., Ibrahim, N. Z. M., & Othman, A. A. (2026). Advancing halal supply chain practices through sustainable innovation transparency and regulatory compliance. *Veredas do Direito*, 23(4), e234736. <https://doi.org/10.18623/rvd.v23.n4.4736>
- Yusof, M. S., Kamarudin, M. A. I., Wahid, A., & Osman, M. F. (2025a). The impact of digital transformation: An empirical analysis on the stability of agro-food SMEs. *International Journal of Business and Technology Management*, 7(6), 287–301. <https://doi.org/10.55057/ijbtm.2025.7.6.24>

- Yusof, M. S., Kamarudin, M. A. I., Wahid, A., & Osman, M. F. (2025b). Transforming agro-food SMEs in Malaysia through digital innovation and smart technologies for sustainable competitiveness. *International Journal of Environmental Sciences*, 11(9s), 530–543.
- Yusof, M. S., Salleh, M. N., & Zahari, F. M. (2020). The relationship between information technology capability and new product development success: A conceptual framework. *International Journal of Business and Technology Management*, 2(1), 98–112.
- Yusof, M. S., Syed A Rahman, S. N. M., Abu Seman, S., & Mohd Zahari, F. (2025). The impact of warehouse management systems on supply chain resilience and business competitiveness in a rapidly changing global market. *International Journal of Business and Technology Management*, 7(2), 332–345. <https://doi.org/10.55057/ijbtm.2025.7.2.30>
- Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: State-of-the-art and research challenges. *Journal of Internet Services and Applications*, 1, 7–18. <https://doi.org/10.1007/s13174-010-0007-6>
- Zhen, L., & Li, H. (2022). A literature review of smart warehouse operations management. *Frontiers of Engineering Management*, 9, 31–55. <https://doi.org/10.1007/s42524-021-0178-9>