computers

MDPI

Article

A Security-Centric Warehouse Management Framework for Mitigating Product Abuse and Cybersecurity Risks

Alparslan Sari [1] **and Ismail Butun** [2,3,*]

[1] Department of Electrical and Computer Engineering, University of Delaware, Newark, DE 19716, USA; asari@udel.edu
[2] Department of Software Engineering, Sakarya University, Serdivan 54050, Türkiye
[3] Research, Development and Application Center (SARGEM), Sakarya University, Esentepe Campus, Serdivan 54050, Türkiye
* Correspondence: ibutun@sakarya.edu.tr; Tel.: +90-264-295-5529

Abstract

This study investigates product abuse, reconciliation challenges, and cybersecurity risks in warehouse management systems (WMS) within increasingly digitized supply chain environments. As warehouses evolve into data-driven operational hubs, vulnerabilities such as data manipulation, insider threats, and fraudulent activities pose significant risks to financial accountability and system integrity. To address these challenges, this research proposes a security-centric WMS framework that integrates blockchain-based immutable logging, Internet of Things (IoT)-enabled tracking, and artificial intelligence (AI)-driven anomaly detection. The methodology follows a hybrid iterative–incremental development approach, supported by real-world deployment of a prototype WMS implemented using a scalable microservices architecture. Over a five-year operational period, the system processed more than 10 million transactions with no recorded successful cybersecurity incidents leading to data breaches, operational compromise, or unauthorized system access, while achieving improvements in reconciliation accuracy, operational efficiency, and fraud detection capabilities. Results demonstrate reductions in manual reconciliation efforts, mispricing incidents, and operational losses, while maintaining high system availability and low latency. In addition, the reported 18–22% improvement associated with AI-assisted anomaly detection is presented as a simulation-based projection rather than a production-validated measurement. The findings indicate that combining secure software engineering practices with automation, auditability, and advanced analytics can significantly enhance transparency and resilience in warehouse operations. The study concludes that integrating decentralized and intelligent technologies provides a viable pathway toward secure, privacy-preserving, and abuse-resistant warehouse ecosystems.

Keywords: warehouse management systems (WMS); product abuse; supply chain security; blockchain integration; Industrial Internet of Things (IIoT); AI-based anomaly detection; auditability

Academic Editor: Raman Singh

Received: 20 April 2026
Revised: 19 May 2026
Accepted: 21 May 2026
Published: 29 May 2026

1. Introduction

Logistics has played a fundamental role in the progression of human societies by ensuring the effective distribution of resources and mitigating risks associated with scarcity. With the shift from conventional trade practices to digital commerce platforms, the demand for efficient and optimized supply chain processes has grown significantly, particularly in the context of warehouse management. In contemporary commerce, warehouses serve as

essential operational hubs where efficiency has a direct impact on profitability, customer experience, and the overall stability of global supply networks.

At the same time, the expansion of digital infrastructures has introduced new challenges for warehouse operations, including risks related to product misuse, data manipulation, and cybersecurity incidents [1,2]. Managing inbound logistics, inventory handling, order fulfillment, and outbound distribution requires strong mechanisms for traceability, reconciliation, and accountability to minimize financial discrepancies and operational conflicts. This challenge becomes more pronounced in modern e-commerce environments, where multi-warehouse fulfillment strategies are increasingly used to reduce order splitting, improve inventory allocation, and optimize logistics efficiency across geographically distributed warehouse networks [3]. Such distributed models increase operational complexity and amplify cybersecurity challenges related to warehouse synchronization, inventory consistency, and cross-facility transaction integrity. When warehouse management systems (WMS) lack sufficient security and transparency, they become susceptible to exploitation by both internal personnel and external adversaries.

1.1. Product Abuse in Warehouse Environments

Product abuse can be defined as the deliberate exploitation or manipulation of warehouse operations and systems for fraudulent or malicious gain. In warehouse settings, such abuse can take multiple forms:

- Supplier-related abuse:intentional or unintentional discrepancies in delivered quantities, substitution of goods, or manipulation of shipment documentation.
- Customer-related disputes: allegations of missing or altered items, often arising from the lack of immutable and verifiable audit trails.
- Insider risks: unauthorized removal of inventory, alteration of system records, or coordinated activities with external parties.
- Data confidentiality breaches: illicit access to sensitive warehouse management system (WMS) information, such as sourcing details, pricing structures, and logistics history, which may be leveraged for competitive advantage.

Conventional reconciliation approaches, including manual verification procedures and enterprise resource planning (ERP) systems, frequently fall short in providing adequate security guarantees to mitigate such risks. Commonly used shared digital tools, such as spreadsheets or inadequately secured WMS platforms, remain vulnerable to unauthorized alterations and intentional data manipulation [4].

1.2. Challenges of Reconciliation and Accountability

Reconciliation—the process of verifying that received goods align with corresponding purchase orders and addressing inconsistencies in a fair manner—continues to represent a significant challenge in warehouse operations. Discrepancies may stem from various sources, including intentional short shipments by suppliers, losses incurred during transportation, or internal theft within warehouse facilities [1].

Accountability further complicates inbound logistics processes. Deliveries are often handled by third-party logistics providers, such as FedEx or UPS, introducing additional layers of uncertainty. When items are missing, it becomes challenging to determine whether the loss occurred during transit, at the point of unloading, or within storage operations. Without mechanisms such as tamper-resistant logging and real-time visibility, disputes among suppliers, carriers, and warehouse operators can intensify, potentially leading to both financial losses and reputational harm. As depicted in Figure 1, product abuse may arise at multiple stages of the supply chain, spanning supplier, transportation, and warehouse domains.

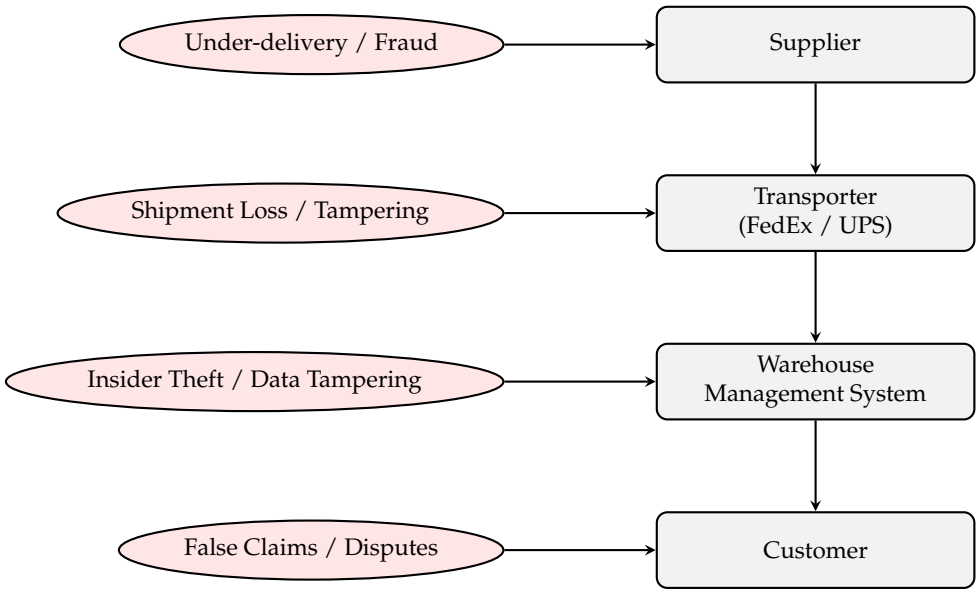

Figure 1. Product abuse and cybersecurity scenarios across the warehouse supply chain [5].

1.3. Security and Cyber Abuse Scenarios

Cybersecurity is critical across industrial and IoT-enabled domains, particularly for protecting both data at rest and data in transit [6]. In addition to financial and operational disputes, warehouse environments are also becoming increasingly vulnerable to cybersecurity threats. Contemporary warehouse management systems (WMS) rely on highly interconnected digital ecosystems and Internet of Things (IoT) technologies—such as RFID systems, handheld scanners, and surveillance sensors—which substantially broaden the potential attack surface. Malicious actors may leverage these vulnerabilities to:

- Alter inventory data to obscure unauthorized removal of goods.
- Insert falsified records that initiate illegitimate financial transactions.
- Compromise IoT devices to conduct denial-of-service attacks or interfere with system integrity.
- Extract sensitive operational data for competitive advantage or illicit use.

These scenarios illustrate the twofold nature of abuse in modern warehouse systems: **operational abuse**, encompassing activities such as theft, fraud, and disputed deliveries, and **cyber abuse**, which includes data manipulation and system-level compromise. As warehouse infrastructures become more digitized and interconnected, these forms of abuse are increasingly interdependent and difficult to isolate.

This risk profile is consistent with recent work on highly automated warehouse systems (HAWS), which identifies cyberattacks, technology sabotage, technology failures, power and network outages, and human–machine interaction failures as the principal technology-related disruption classes affecting automated warehouse environments [7]. In particular, the increasing reliance on cloud-based WMS/WCS platforms, IoT devices, AMRs/AGVs, robotics, and multi-vendor automation networks expands the warehouse attack surface and creates the possibility that a localized software, network, or supplier vulnerability may cascade into operational downtime, inventory inaccessibility, or supply-chain-wide disruption [7].

1.4. Blockchain- and IoT-Based Mitigation Strategies

Emerging technological paradigms, including blockchain, Internet of Things (IoT), and AI-based anomaly detection, offer promising solutions to address product abuse within warehouse environments.

- **Blockchain for immutable record-keeping**: The use of blockchain enables the creation of tamper-resistant transaction logs, ensuring that once inventory-related data are recorded, they cannot be modified or removed. This enhances transparency and accountability by allowing all participating entities—such as suppliers, warehouse operators, and customers—to independently validate records without depending on a centralized authority [4].
- **Smart contracts for automated reconciliation**: By embedding business logic into blockchain-based smart contracts, reconciliation and payment processes can be executed automatically. Payments are conditionally released only after successful verification of delivery, thereby reducing disputes associated with manual validation procedures.
- **IoT-driven traceability and monitoring**: Integration of IoT devices, including RFID tags, surveillance systems, and environmental sensors, with warehouse management systems facilitates continuous, real-time monitoring of shipments. Events such as package handling, transit tracking, and environmental changes collectively establish a verifiable chain of custody, limiting opportunities for tampering or loss.
- **AI-based anomaly detection**: Advanced machine learning techniques can analyze logistics and inventory data to detect unusual patterns, such as irregular product movements or inconsistent delivery reports. These systems can proactively generate alerts, enabling timely investigation and mitigation of potential abuse scenarios.

1.5. Beyond DSS: Security as a Core Priority

Decision Support Systems (DSS) have historically been utilized to enhance operational efficiency in warehouse environments, particularly in areas such as workforce planning, scheduling, and resource allocation. However, their role in mitigating **cybersecurity risks and product abuse** has been comparatively limited. While operational optimization remains important, it is subordinate to critical concerns such as fraud prevention, data integrity assurance, and protection of sensitive information. Consequently, a cybersecurity-centric design paradigm is required for next-generation warehouse management systems (WMS), in which DSS functions as a supporting analytical tool rather than the primary focus.

1.6. Contributions

This study investigates **product abuse and cybersecurity risks within warehouse management systems**, addressing both operational inefficiencies and digital security vulnerabilities. To mitigate these challenges, it introduces an integrated framework that leverages **blockchain technology, IoT-based tracking, and AI-enabled anomaly detection** to improve transparency, security, and system-wide accountability. The primary contributions of this work are summarized as follows:

- **Characterization of warehouse-specific abuse vectors**, including supplier-side fraud, customer-driven disputes, insider manipulation, and violations of data confidentiality.
- **Critical evaluation of reconciliation and accountability gaps** in existing warehouse management practices and systems.
- **Design of blockchain- and IoT-enabled mitigation strategies** to support secure, tamper-resistant data recording and traceability.
- **Integration of AI-based anomaly detection techniques** to identify irregular patterns and proactively flag potential fraudulent or malicious activities.

By addressing these dimensions, the proposed framework aims to strengthen trust among stakeholders, minimize financial and operational risks, and advance the development of robust and fraud-resilient warehouse management ecosystems.

2. Related Work

2.1. Operational WMS, IIoT, and Automation

Warehouse management research has historically focused on operational efficiency, inventory accuracy, order fulfillment, storage optimization, and decision support. Early warehouse management and decision-support studies examined how structured software systems, inventory-control methods, and operational planning tools could improve warehouse throughput, resource allocation, and process visibility [1]. Conventional WMS and DSS-oriented approaches have contributed significantly to warehouse modernization; however, they have generally emphasized productivity and optimization more than cybersecurity, product abuse prevention, immutable auditability, or privacy-preserving accountability.

Operational warehouse literature has also emphasized that successful warehouse transformation depends not only on software deployment, but also on KPI-driven governance, organizational readiness, sustainability evaluation, implementation planning, ERP integration, workforce training, and long-term operational monitoring [8–10]. Prior studies show that modernization efforts benefit from multidimensional evaluation frameworks incorporating inventory accuracy, operational throughput, sustainability indicators, workforce considerations, implementation governance, and periodic system audits. These findings suggest that effective WMS deployment should be treated as an organizational transformation process rather than a purely technical implementation effort.

Within this broader transformation, IIoT-enabled warehouse architectures have become central to improving real-time visibility, inventory synchronization, safety monitoring, and decision-support capabilities. Prior studies demonstrated that RFID readers, environmental sensors, connected forklifts, cloud-based analytics platforms, barcode-enabled workflows, and Real-Time Location Systems (RTLS) can substantially improve inventory tracking, warehouse monitoring, operational safety, and data-driven decision-making [11–13]. These technologies enable continuous monitoring of warehouse activities, reduce manual processing errors, improve traceability across receiving, putaway, picking, outbound validation, loading, and stock reconciliation processes, and support real-time detection of congestion, unsafe forklift behaviors, routing inefficiencies, and operational bottlenecks.

Earlier IoT-enabled WMS studies provide additional foundation for this direction. Lee et al. [14] demonstrated the use of real-time industrial data in an IoT-based WMS, while Čolaković et al. [15] surveyed enabling technologies for smart warehouse monitoring. Domain-specific RFID applications, such as intelligent drug-management cabinets, further show that RFID-based traceability can improve operational control in specialized warehouse contexts [16]. However, these studies primarily emphasize sensing, monitoring, and process visibility; without cryptographic safeguards, privacy-aware access control, and immutable auditing, such systems remain vulnerable to data manipulation, unauthorized access, and disputed reconciliation outcomes.

In parallel, automation and intelligent optimization techniques have become important enablers of modern e-commerce and large-scale logistics operations. Prior research highlights the role of autonomous mobile robots (AMRs), automated guided vehicles (AGVs), goods-to-person (G2P) systems, automated storage and retrieval systems (AS/RS), barcode-driven automation, and AI-based optimization in improving warehouse throughput, order fulfillment speed, labor productivity, inventory accuracy, and operational scalability [17,18]. Genetic algorithm-based warehouse optimization frameworks further demonstrate that product placement and order-picking routes can be optimized using historical order patterns, thereby reducing picking costs, route completion times, and operational inefficiencies in large warehouse environments.

2.2. Smart Warehouses, Digital Twins, AI, and Human-Centered Interfaces

Recent bibliometric and trend-analysis studies further demonstrate that warehouse research has increasingly evolved toward smart, data-driven, and cyber–physical ecosystems integrating Industry 4.0 technologies such as IoT, AI, machine learning, robotics, RFID, blockchain, automation, and advanced analytics [19,20]. These studies collectively indicate a broader transition from conventional warehouse software toward intelligent and interconnected warehouse infrastructures capable of supporting real-time monitoring, predictive analytics, operational automation, and enhanced supply chain transparency. This evolution aligns with the positioning of the proposed framework, which combines blockchain-enabled auditability, IoT-driven operational visibility, and AI-assisted anomaly detection to strengthen accountability and cybersecurity resilience within warehouse management systems.

Recent studies on warehouse management in connectivity-constrained industrial environments additionally demonstrate that offline-first system architectures can improve operational continuity and data consistency during network outages [21]. Progressive Web Application (PWA)-based warehouse systems using local persistence, synchronization queues, and conflict-resolution mechanisms have shown reliable operation even when a substantial portion of warehouse transactions occur offline. These findings reinforce the importance of resilient synchronization strategies, local caching, and distributed transaction management for IIoT-enabled warehouse ecosystems operating under unstable connectivity conditions.

Closely related to resilience, compliance-oriented warehouse management research highlights the importance of embedding regulatory enforcement directly into operational workflows [22]. In bonded warehouse environments, web-based inventory systems combined with automated gate control, centralized master data management, and real-time customs verification mechanisms have reduced reporting delays and data-entry errors while improving traceability and operational transparency. This demonstrates that warehouse systems are increasingly expected to transform traditionally reactive audit processes into proactive governance mechanisms, aligning with the broader objectives of accountable and resilient IIoT-enabled warehouse ecosystems.

At the strategic level, Warehousing 5.0 and Green Warehouse 5.0 research expand the conceptual foundation of intelligent warehouse ecosystems by emphasizing human-centric design, AI-enabled automation, sustainability, resilience, digital transformation, and cyber-resilient operations [23,24]. These perspectives suggest that next-generation warehouses should not be viewed solely as productivity-driven infrastructures, but as adaptive socio-technical ecosystems that integrate human well-being, environmental sustainability, ethical data governance, responsible AI, human–robot collaboration, and resilient digital governance into operational decision-making. This framing is also important because highly automated warehouse environments may introduce worker-monitoring, surveillance, and accountability concerns alongside operational optimization objectives [25].

This strategic interpretation is reinforced by research on automated warehouse systems, which positions warehouse platforms as long-term organizational infrastructure rather than isolated operational tools [26]. Automation decisions are shaped not only by throughput, cost, and order accuracy, but also by strategic intent, scalability, technology-supplier relationships, control and ownership, risk exposure, and robustness. This perspective is directly relevant to security-centric WMS design because cybersecurity controls, auditability, access governance, and resilience mechanisms should be evaluated as part of warehouse automation strategy rather than treated as late-stage technical add-ons.

Digital twin technologies have also emerged as an important mechanism for improving operational visibility, sustainability, simulation, and adaptive decision-making in warehouse management systems [27–30]. Digital twins enable synchronization between

physical warehouse operations and virtual monitoring environments, supporting predictive analysis, resource optimization, operational simulation, and performance management. From a cybersecurity perspective, digital twins may also enhance anomaly detection and operational auditing by providing continuous behavioral baselines for warehouse assets, workflows, and cyber–physical interactions.

Recent AI-oriented warehouse studies further demonstrate that intelligent monitoring and decision-support capabilities can be deployed in practical warehouse environments. Compact multimodal AI architectures such as SmolRGPT integrate RGB and depth cues for warehouse-oriented spatial reasoning while remaining suitable for resource-constrained edge environments [31]. Similarly, machine-learning surveys show that predictive analytics, supervised learning, unsupervised learning, optimization models, and decision-support methods are increasingly used for demand forecasting, storage assignment, picking optimization, anomaly detection, and operational planning [32]. These findings support the view that WMS data should be treated as an operational intelligence layer rather than merely as transactional inventory records.

AI-driven warehouse and supply chain security research further indicates that automation benefits must be evaluated together with cybersecurity risk. Sodiya et al. [33] emphasize that AI-enabled warehouse automation can improve efficiency while also increasing exposure to security risks in interconnected environments. Similarly, Hern'andez et al. [34] examine collaborative intelligence mechanisms for end-to-end cybersecurity monitoring across global supply chain networks. These studies reinforce the need to pair AI-enabled optimization with threat detection, abuse mitigation, and security-aware governance mechanisms.

Human-centered intelligent warehouse interfaces have also gained attention. Research on AR-assisted indoor navigation, voice-driven interaction, mixed-reality interfaces, and large language model (LLM)-based assistants demonstrates how emerging technologies can support operator guidance, hands-free task execution, contextual decision support, and human–AI collaboration in warehouse environments [35–38]. These studies show that future WMS platforms may increasingly combine operational data, semantic reasoning, and user-centered interfaces to reduce cognitive load and improve real-time coordination. However, they also highlight practical concerns related to reliability, calibration, noisy environments, safety, and integration with existing warehouse systems.

Increasing automation density introduces additional operational and organizational complexity. Studies on multi-deep rack systems, AI-based order picking, automated stocktaking, warehouse layout optimization, and predictive warehouse design demonstrate that storage density, routing, picking accuracy, item retrieval, and operational scalability are interdependent challenges [39–43]. While these studies report improvements in efficiency and productivity, they also identify barriers such as infrastructure cost, workforce adaptation, legacy-system integration, cybersecurity concerns, and organizational resistance. These findings reinforce the need for warehouse intelligence frameworks that balance technological innovation with practical deployment constraints, employee acceptance, cybersecurity governance, and long-term maintainability.

Robotics and autonomous warehouse systems represent another major research stream. Reviews and case studies show that AMRs, AGVs, drones, robotic material-handling systems, reinforcement learning-based navigation, task scheduling, and autonomous pallet handling can support picking, replenishment, transport, inventory inspection, stocktaking, and robotic manipulation [44–50]. These technologies strengthen warehouse automation and scalability, but they also increase dependence on reliable sensing, secure coordination, cyber–physical safety, and resilient integration with WMS platforms.

Sustainability-oriented warehouse research further shows that WMS platforms increasingly contribute to environmental responsibility, resource optimization, energy efficiency,

waste reduction, and socially responsible logistics practices [51–53]. Data-driven optimization frameworks integrating renewable energy, energy storage, microgrid systems, and automated storage and retrieval systems indicate that warehouse scheduling decisions can influence energy consumption and carbon emissions. These findings support the need to evaluate intelligent WMS architectures not only through operational and financial metrics, but also through sustainability and governance dimensions.

Lean warehousing and process-optimization studies also remain relevant to smart warehouse transformation. Research using Lean Six Sigma, value stream mapping, Gemba walks, discrete-event simulation, layout redesign, ABC/XYZ categorization, and workflow standardization demonstrates that process mapping and simulation can reduce non-value-added time, improve throughput, identify bottlenecks, and enhance ergonomic conditions [54–59]. These studies support the practical importance of combining software-enabled monitoring with continuous improvement methods.

Structured Warehouse Management Information System (WMIS) and database-centered WMS research further demonstrates the value of centralized and computerized warehouse architectures for improving inventory control, raw material tracking, production coordination, transaction management, and operational reporting [60–62]. Such systems reduce manual inventory errors and improve warehouse process visibility through integrated software design and database-driven orchestration. However, while these systems improve operational control, they generally remain focused on process efficiency and reporting rather than cybersecurity, immutable auditability, privacy-preserving access control, or abuse-resistant reconciliation.

Recent systematic reviews on cold-storage warehouse management systems further show that successful WMS deployments require simultaneous consideration of technical infrastructure, organizational readiness, integration complexity, interoperability, and human factors such as workforce training, resistance to change, and user adoption [63]. These challenges become even more significant in warehouse ecosystems that depend on interconnected APIs, IoT-enabled temperature-control systems, real-time monitoring platforms, and digitally integrated supply chain operations.

2.3. Blockchain-Based Accountability and Smart Contract Verification

Blockchain-based supply chain and warehouse studies have begun to address some of these accountability limitations. Recent work on blockchain-enabled warehouse receipt systems demonstrates that multi-chain architectures, smart-contract-driven automation, layered data protection, and cross-chain verification mechanisms can support secure multi-party collaboration, data isolation, and interoperability across heterogeneous supply chain actors [64]. These findings are relevant to warehouse reconciliation because disputes often involve multiple parties, including suppliers, logistics providers, warehouse operators, and customers. Nevertheless, real-world blockchain deployment remains challenging due to stakeholder onboarding, governance, interoperability, smart contract standardization, and integration with proprietary external systems.

Smart contract design is particularly important in warehouse reconciliation because multiple warehouse events may share common validation requirements while still requiring event-specific logic. For example, inbound shipment registration, package-level verification, supplier confirmation, discrepancy reporting, reconciliation approval, and payment release may all require validation of actor identity, transaction consistency, fulfillment conditions, asset state, and approval status. Reusable smart contract design approaches, such as AdapT, provide useful guidance for implementing smart contracts that process related transaction categories using configurable verification rules [65]. This supports the interpretation of

blockchain not merely as immutable storage, but as a programmable verification layer for warehouse accountability.

2.4. Cybersecurity Gaps in Highly Automated Warehouse Systems

Cybersecurity-focused industrial systems research further supports the need for secure, distributed, and resilient architectures. Fog computing has been recognized as an effective paradigm for improving security, performance, and scalability in IoT environments by reducing latency, decentralizing processing, and limiting exposure of sensitive data [66,67]. Related work on early threat detection and recovery for cyber-resilient industrial systems also emphasizes the importance of anomaly detection, edge-based security controls, and intrusion prevention mechanisms [68]. These concepts are directly applicable to warehouse management systems, where secure access control, reliable operation, and low-latency monitoring are essential.

Recent research on highly automated warehouse systems (HAWS) further shows that smart warehouses should be treated as cyber–physical systems exposed to cyberattacks, technology sabotage, technology failures, power and network outages, and human–machine interaction disruptions [7]. This perspective broadens the threat model beyond conventional web vulnerabilities by emphasizing software systems, data management, automation hardware, digital networks, physical infrastructure, organizational factors, and operational vulnerabilities. It is directly relevant to the proposed WMS framework because warehouse abuse may emerge from both digital compromise and physical operational manipulation.

Overall, the literature demonstrates strong progress in WMS deployment, IIoT-enabled visibility, automation, robotics, digital twins, AI-assisted optimization, sustainability, and smart warehouse transformation. However, existing studies still provide comparatively limited treatment of product abuse, insider threats, immutable auditability, privacy-preserving access control, smart-contract-based reconciliation, and cybersecurity-aware warehouse accountability. This gap motivates the present study, which proposes a security-centric WMS framework integrating secure software engineering practices, blockchain-enabled auditability, IoT/RFID-based traceability, and AI-assisted anomaly detection to mitigate abuse and strengthen trust in warehouse operations.

3. Problem Analysis and Key Issues

Modern warehouse operations are increasingly dependent on digital infrastructures; however, they continue to encounter significant challenges that impact operational efficiency, system security, and financial accountability. These challenges stem from a combination of software weaknesses, inadequate security controls, and process inefficiencies, which may result in financial losses, data breaches, and erosion of stakeholder trust. Effectively addressing these concerns requires a comprehensive evaluation of risks related to software systems, cybersecurity threats, and potential abuse scenarios within warehouse management systems (WMS).

Accordingly, the threat model considered in this study is broadened beyond conventional web-application vulnerabilities to include the technology-related disruption categories reported for HAWS: cyberattacks, technology sabotage, technology failures, power and network outages, and human–machine interaction failures [7]. This broader view strengthens the motivation for combining secure APIs, RBAC/MFA, auditability, IoT/RFID traceability, and future blockchain-based immutability, because warehouse disruption risk arises from both digital compromise and cyber–physical operational dependencies.

Through an examination of prevalent security threats, reconciliation complexities, and risks to data integrity, this section highlights the fundamental limitations of current warehouse management approaches. The insights derived from this analysis establish the

groundwork for the development of blockchain-enabled solutions designed to enhance transparency, strengthen fraud detection capabilities, and ensure privacy preservation.

3.1. Software and Cybersecurity Vulnerabilities

Deficiencies in warehouse management system (WMS) software can introduce operational inefficiencies, financial inconsistencies, and exploitable security weaknesses. Issues such as poor coding practices, inadequate authentication controls, and insufficient input validation increase the risk of system manipulation and fraudulent activities. Additionally, systems that are not designed with scalability in mind may struggle to accommodate growing operational demands, leading to performance degradation and potential service interruptions. Addressing these concerns necessitates adherence to robust software engineering standards, ongoing security assessments, and the adoption of comprehensive cybersecurity frameworks to ensure data integrity, reliability, and confidentiality.

Errors at the implementation level can also result in tangible financial impacts. For example, the use of integer data types instead of floating-point or high-precision representations for monetary values may introduce rounding inaccuracies in financial transactions, potentially causing overbilling or underbilling. Such discrepancies not only undermine customer confidence but may also be exploited by malicious insiders to obscure fraudulent activities.

With the increasing adoption of digital record-keeping and automated processes, warehouse systems have become more attractive targets for cyber threats. Among the most common attack vectors are **Cross-Site Scripting (XSS)** and **SQL Injection (SQLi)**, both of which can facilitate unauthorized system access, data exfiltration, and financial exploitation.

3.1.1. Protection Against XSS and SQL Injection

Cross-Site Scripting (XSS) attacks target client-side vulnerabilities by injecting malicious scripts into web content that is subsequently rendered in users' browsers. Through such attacks, adversaries can capture session tokens, alter the integrity of displayed information, or redirect users to malicious domains. Mitigation of XSS vulnerabilities requires the implementation of the following measures:

1. All user-supplied inputs should undergo thorough sanitization and appropriate encoding prior to being rendered in the browser.
2. A robust Content Security Policy (CSP) must be implemented to limit the execution of unauthorized or untrusted scripts.
3. Effective output encoding and escaping mechanisms should be applied to mitigate the risk of HTML or script injection.

SQL Injection (SQLi) attacks arise when adversaries exploit insufficient input validation to manipulate database queries, thereby enabling unauthorized access to sensitive information such as customer records or inventory data. Effective mitigation of SQLi vulnerabilities requires the following measures:

1. Database interactions should utilize parameterized queries or prepared statements to securely handle user-provided inputs.
2. The use of direct string concatenation when constructing SQL queries with user input must be strictly avoided.
3. Role-based access control (RBAC) mechanisms should be implemented to limit privileges and prevent unauthorized data modifications.

3.1.2. Secure Authentication and Authorization

Multi-Factor Authentication (MFA) strengthens authentication mechanisms by requiring users to provide additional forms of verification beyond traditional passwords. Techniques such as rate limiting and brute-force mitigation further reduce the risk of cre-

dential stuffing and unauthorized access attempts. In addition, robust session management practices—including token expiration policies, automatic session termination, and secure invalidation procedures—are essential for minimizing the likelihood of session hijacking.

3.1.3. Data Validation and API Security

Insecure API endpoints represent significant threats to both data privacy and system integrity. Many warehouse management system (WMS) interfaces can be examined and manipulated through browser-based developer tools, making them vulnerable to unauthorized access and parameter tampering. It is imperative that users are prevented from accessing other customers' data by modifying request parameters. Accordingly, backend systems must enforce strict validation of both request origin and data ownership. In the absence of such controls, adversaries may gain access to confidential inventory information, generate fraudulent transactions, or overwhelm systems with fabricated requests.

To mitigate these risks, API endpoints should incorporate robust authentication and authorization mechanisms, secure communication protocols (e.g., TLS for data in transit and AES-256 for data at rest), and rate-limiting strategies combined with comprehensive request logging for anomaly detection. These measures are critical for maintaining data confidentiality, ensuring integrity, and enhancing the overall resilience of warehouse management systems.

3.1.4. Secure Software Development Lifecycle (SDLC)

Security considerations should be integrated across the entire software development lifecycle. Practices such as systematic code reviews and automated vulnerability scanning support the early identification of potential weaknesses, while effective patch management ensures that third-party components remain up to date and secure. Collectively, these measures promote a proactive security posture, reduce exposure to zero-day vulnerabilities, and facilitate adherence to established industry standards.

3.2. Product Abuse in WMS

Even when software systems are technically robust, **product abuse and operational manipulation** continue to pose significant risks. A key source of revenue in warehouse operations is derived from services such as repackaging and product handling, where pricing is typically determined by factors including volume, service frequency, and service-level agreements [69]. Since pricing structures often vary across customers, accurate cost allocation becomes critically important. Any deviation from precise accounting—whether due to oversight, human error, or intentional misconduct—can lead to considerable financial inconsistencies.

A common challenge in warehouse operations is **inaccurate billing practices**, often associated with high workforce turnover. Newly onboarded employees may receive limited training on WMS functionalities, which increases the likelihood of both unintentional errors and deliberate misuse.

Common abuse scenarios include:

1. **Customer overbilling**: The application of excessive service charges or duplicate billing entries can result in financial harm to customers. Such issues may arise from manual data entry mistakes, incorrect pricing configurations, or intentional manipulation of records.
2. **Customer underbilling**: The omission or misapplication of appropriate fees leads to revenue loss for warehouse operators. This is often attributable to insufficient training, misinterpretation of pricing structures, or, in some cases, coordinated misconduct.
3. **Challenges in order reconciliation and accountability**: Errors such as incorrect inventory labeling, fabricated shortage claims, or internal theft can create substantial

discrepancies. In the absence of immutable and verifiable audit mechanisms, these irregularities may go undetected.

These observations indicate that **cybersecurity vulnerabilities and product abuse often originate from shared underlying factors**, including limited auditability, the lack of tamper-resistant logging mechanisms, and insufficient anomaly detection capabilities. As warehouse management systems (WMS) transition into increasingly interconnected digital ecosystems, both technical weaknesses and human factors can be leveraged by malicious actors. Accordingly, the development of **secure, transparent, and verifiable transaction frameworks** has become a critical requirement.

Blockchain-enabled logging, privacy-aware IoT tracking, and AI-based anomaly detection together establish a comprehensive foundation for addressing these challenges. By preserving data integrity, strengthening accountability, and facilitating the early identification of anomalous activities, these approaches have the potential to shift warehouse management from a trust-dependent model toward a **security-driven and abuse-resilient ecosystem**.

4. Proposed Solutions and Framework

To improve security, privacy, and data integrity within warehouse management systems (WMS), this section introduces a comprehensive framework aimed at preventing unauthorized access, mitigating data breaches, and reducing fraudulent activities, including product abuse. The proposed approach integrates automated processes, blockchain-based reconciliation, rigorous API validation, and Zero Trust security principles to establish strong access control, ensure data confidentiality, and promote operational transparency.

4.1. Automation for Error Prevention

An effective warehouse management system (WMS) should reduce human-induced errors by automating all billing and charge computations based on predefined contractual agreements. Manual input should be restricted primarily to validation and oversight functions, while pricing rules are systematically enforced through encoded logic within the system. Such automation minimizes inconsistencies arising from human oversight and limits opportunities for intentional manipulation, thereby ensuring financial accuracy and consistent application of business policies.

4.2. Audit Transactions for Financial Accuracy

Periodic financial and operational audits play a critical role in identifying pricing inconsistencies and uncovering potential fraudulent activities. Annual processing records should be systematically evaluated against projected revenue benchmarks to generate automated discrepancy reports, particularly at the item level. This approach improves transparency, facilitates continuous performance assessment, and enables proactive detection of anomalies within warehouse management systems (WMS).

4.3. Blockchain for Immutable Record Keeping

The integration of blockchain technology into warehouse management systems (WMS) enables the creation of tamper-resistant and verifiable transaction records. Each operational event—such as item processing, applied charges, and customer billing—can be securely recorded on an immutable ledger, preventing unauthorized modifications. This capability ensures the integrity of order, pricing, and inventory data, thereby simplifying reconciliation processes and reducing the likelihood of disputes.

The inherent transparency and auditability of blockchain systems facilitate more efficient dispute resolution, as all stakeholders—including customers, warehouse operators, and logistics providers—can independently validate transaction histories through cryp-

tographic evidence. In addition, smart contracts enhance accountability by automating business logic, ensuring that payments are executed only after confirmed fulfillment of delivery conditions.

Adopting a **permissioned blockchain** architecture further supports privacy and controlled collaboration within the supply chain by limiting network participation to authorized entities, such as suppliers, buyers, carriers, and warehouse operators. This approach preserves transparency while protecting sensitive operational and commercial data from unauthorized disclosure.

From a design perspective, the smart contract component shown in the proposed framework should support reusable transaction verification rather than hard-coded validation logic for each warehouse event type. AdapT provides a relevant design reference because it separates generic smart contract abstractions from concrete transaction-specific rules and enables verification-rule reuse across congruous transaction types [65]. This approach is applicable to warehouse reconciliation workflows, where different events such as inbound receiving, discrepancy reporting, shipment validation, and payment authorization may share common verification requirements while requiring different rule configurations.

4.4. Securing Internal API Dynamics

Internal APIs should be segregated from external access wherever feasible to reduce exposure to potential threats. All API communications must incorporate token-based authentication mechanisms (e.g., OAuth 2.0 or JSON Web Tokens (JWT)) to ensure that only authorized and authenticated entities can access protected resources. Furthermore, the implementation of **role-based access control (RBAC)** enables fine-grained permission management, restricting users to only the data and operations associated with their designated roles.

4.5. Backend Validation to Prevent Malicious Requests

All API requests must be subjected to rigorous backend validation prior to any data processing or system execution. Techniques such as input sanitization and strict parameter validation are essential to defend against **SQL Injection (SQLi)**, **Cross-Site Scripting (XSS)**, and malicious payload manipulation. In addition, mechanisms such as rate limiting and anomaly detection should be employed to analyze request frequency and behavioral patterns, enabling the identification and mitigation of suspicious activities, including brute-force attacks.

4.6. Preventing Unauthorized Data Access and Privacy Violations

Ensuring data isolation and enforcing ownership validation are essential for preserving privacy within warehouse management systems. Under no circumstances should a customer be able to access another customer's sensitive information, including dashboards, billing records, or analytical reports. Access control policies must therefore enforce strict scoping, limiting data visibility based on authenticated user identity.

For instance, in an API structured as `/inventory/:customerid`, modifying the `customerid` parameter should not permit unauthorized data access. Instead, backend systems must rely on token-based identity verification to confirm data ownership before fulfilling any request. Such enforcement mechanisms prevent data leakage and maintain strict segregation of customer information, thereby safeguarding confidential business data.

4.7. Protecting Payment and Order Processing Workflows

All payment and order processing activities must be strictly validated against authenticated user accounts to mitigate the risk of financial fraud. Systems should be designed to prevent adversaries from redirecting payments or altering order workflows. The use

of blockchain-supported transaction logging provides transparent and immutable audit trails for financial operations, thereby strengthening accountability and facilitating efficient reconciliation.

4.8. API Security Best Practices

Effective API security practices are essential for defending against prevalent cybersecurity threats:

- Utilize **HTTPS/TLS protocols** to secure data in transit and mitigate the risk of Man-in-the-Middle (MITM) attacks.
- Implement **Web Application Firewalls (WAFs)** to detect and block malicious traffic, including API-targeted exploits.
- Establish **continuous monitoring and logging mechanisms** to enable timely detection and response to unauthorized access attempts.

The adoption of these measures strengthens the resilience of warehouse management systems against contemporary cyber threats, while preserving data privacy, ensuring operational integrity, and supporting financial transparency.

4.9. Zero Trust Policy in Warehouse Management

The proposed architecture aligns conceptually with the NIST Zero Trust Architecture (ZTA) principles, where authentication, authorization, and continuous validation are enforced for every user, device, and service interaction regardless of network location [70]. In this model, no internal or external entity is trusted by default, and all access requests are continuously verified prior to resource access.

The implemented security model incorporates JSON Web Token (JWT)-based authentication, Role-Based Access Control (RBAC), and Multi-Factor Authentication (MFA) mechanisms to restrict access according to operational responsibilities. Backend APIs, workflow services, and administrative interfaces operate as policy enforcement points where user identity, token validity, ownership constraints, and authorization policies are validated before execution of any operation.

Continuous monitoring, audit logging, rate limiting, and anomaly detection mechanisms further strengthen the architecture by enabling identification of suspicious access patterns and unauthorized activities. In addition, network segmentation and secure service-to-service communication reduce lateral movement risks within the warehouse ecosystem.

By integrating continuous authentication, comprehensive auditing, and strict access validation, warehouse environments can significantly mitigate risks associated with insider threats, external intrusions, unauthorized data access, and operational abuse scenarios.

4.9.1. Ensuring Accountability in Inbound Shipments

Inbound logistics processes are especially susceptible to risks such as theft, tampering, and fraudulent reporting. For example, a supplier may declare the shipment of 1000 units while only 950 units are actually received, leading to discrepancies, disputes, and financial losses. Traditional manual reconciliation approaches are insufficient to address such high-risk scenarios effectively. These vulnerabilities may arise at various stages of the process:

1. Losses incurred during transportation as a result of mishandling or tampering;
2. Partial diversion or theft occurring at the point of origin prior to dispatch;
3. Deliberate under-shipment or inaccurate quantity reporting by suppliers;
4. Theft during transit involving logistics personnel or external actors;
5. Unauthorized removal of goods at the destination warehouse;
6. Misplacement or inventory errors during storage processes.

4.9.2. Implementing CCTV Surveillance and Proof of Delivery

The deployment of CCTV systems in critical warehouse areas serves both as a deterrent to theft and as a means of maintaining verifiable audit trails for inbound and outbound operations. Recording box-opening procedures enables validation of both the quantity and condition of received goods, with such footage securely stored within encrypted cloud-based infrastructures. Furthermore, the integration of **RFID and IoT-enabled tracking technologies** provides continuous, end-to-end visibility across the supply chain, from origin to final delivery. The use of tamper-evident packaging additionally reinforces physical integrity and reduces the likelihood of undetected interference.

4.9.3. Reducing Human Error in Pricing and Reconciliation

Automation should extend beyond basic computational tasks to include AI-driven reconciliation processes. Machine learning algorithms can continuously analyze expected versus actual inventory levels, enabling near real-time detection of discrepancies. In parallel, blockchain-based audit mechanisms ensure that pricing and transaction data are recorded immutably, thereby enhancing transparency and reducing the potential for manual interference or manipulation.

The integration of **IoT sensors and RFID-based tracking systems** facilitates continuous and tamper-resistant monitoring of goods across the supply chain. These technologies produce timestamped, verifiable data that can be securely recorded on a blockchain ledger, thereby minimizing reconciliation discrepancies and offering reliable evidence in the event of disputes.

AI-based anomaly detection systems can evaluate transactional and behavioral data to identify suspicious or potentially fraudulent activities in real time [68]. In parallel, privacy-preserving surveillance approaches—such as encrypted cloud storage for CCTV footage combined with edge-based analytics—help safeguard sensitive operational data while maintaining effective situational awareness.

To strengthen accountability, delivery records generated by logistics providers should be cryptographically signed and stored within a permissioned blockchain, thereby establishing verifiable proof of delivery and supporting a **reputation-based trust framework** among participating entities. In addition, predictive analytics techniques can be employed to anticipate risks such as shipment losses, fraudulent reporting, or order manipulation, enabling proactive mitigation through automated alerts and dynamic risk scoring mechanisms.

The risk classifications presented in Tables 1 and 2 are based on a **qualitative risk assessment framework** informed by established standards, including ISO 31000 and NIST SP 800-30.

Each identified threat or risk scenario was assessed across two key dimensions: Likelihood (the probability of occurrence) and Impact (the severity of potential consequences), using a five-point ordinal scale where 1 corresponds to Rare/Minor and 5 to Almost Certain/Critical. The overall Risk Level was then categorized as Low, Medium, or High, guided by expert evaluation and empirical evidence drawn from documented warehouse cybersecurity incidents and operational disruptions.

Table 1. Qualitative risk assessment: WMS security threats.

Threat Category	Likelihood	Impact	Risk Level	Primary Mitigation
SQL Injection (SQLi)	4 (Likely)	5 (Critical)	High	Parameterized queries, prepared statements, WAF, RBAC, least privilege DB roles
Cross-Site Scripting (XSS)	5 (Almost Certain)	4 (Major)	High	Input sanitization, output encoding, strict CSP, WAF, secure templating

Table 1. *Cont.*

Threat Category	Likelihood	Impact	Risk Level	Primary Mitigation
Unauthorized API Access	4 (Likely)	5 (Critical)	High	OAuth2/JWT, mTLS, RBAC/ABAC, rate limiting, anomaly detection, comprehensive logging
Insider Misuse/Data Leakage	3 (Possible)	4 (Major)	Medium	Segregation of duties, just-in-time access, immutable audit trails (blockchain), DLP, monitoring
Data Tampering (Records)	4 (Likely)	5 (Critical)	High	Permissioned blockchain logging, integrity checks, append-only storage, dual control
Misconfigured API Exposure	3 (Possible)	4 (Major)	Medium	Secure SDLC, API gateways, schema validation, automated security testing (SAST/DAST)

Scale legend: Likelihood and Impact are scored 1–5 (1 = Rare, 2 = Unlikely, 3 = Possible, 4 = Likely, 5 = Almost Certain; Impact: 1 = Minor … 5 = Critical). Risk Level reflects a qualitative combination of both.

Table 2. Qualitative risk assessment: Logistics and product abuse risks.

Logistics/Abuse Risk	Likelihood	Impact	Risk Level	Primary Mitigation
Inbound Shipment Loss/Tampering	4 (Likely)	5 (Critical)	High	IoT/RFID tracking, tamper-evident packaging, cryptographic Proof of Delivery (PoD), CCTV with encrypted storage, permissioned blockchain logs
Storage Theft (On-site)	3 (Possible)	4 (Major)	Medium	Access controls, CCTV coverage, inventory cycle counts, anomaly alerts on movement, immutable audit trails
Reconciliation Fraud/Pricing Manipulation	4 (Likely)	5 (Critical)	High	Automation of pricing, AI-driven reconciliation, dual approval, blockchain-based billing history
Outbound Shipment Loss	4 (Likely)	4 (Major)	High	Chain-of-custody with RFID/IoT, signed carrier logs, delivery scanning, smart contract gated payment release
False Customer Claims (Non-delivery/Quality)	3 (Possible)	4 (Major)	Medium	Photo/Video PoD, sensor telemetry, verifiable timestamps on blockchain, dispute workflows
Supplier Under shipment/Miscount	3 (Possible)	4 (Major)	Medium	AI variance detection, weigh/measure stations, recorded box opening, shared immutable receiving logs

Scale legend: Likelihood and Impact are scored 1–5 (1 = Rare, 2 = Unlikely, 3 = Possible, 4 = Likely, 5 = Almost Certain; Impact: 1 = Minor … 5 = Critical). Risk Level reflects a qualitative combination of both.

This dual-matrix methodology establishes a structured basis for prioritizing mitigation efforts across both technical and procedural domains.

- Table 1 captures cyber-oriented vulnerabilities, including threats such as SQL injection, Cross-Site Scripting (XSS), and insider misuse, all of which compromise the integrity of WMS digital infrastructures.
- Table 2 examines physical and procedural abuse scenarios—such as shipment tampering, reconciliation fraud, and false reporting—that undermine trust and financial accountability in warehouse operations.

By systematically mapping these categorized risks to their corresponding mitigation strategies—namely blockchain for ensuring data integrity, IoT/RFID technologies for enhancing operational visibility, and AI for anomaly detection—the proposed framework

provides a comprehensive approach that addresses both cyber and physical dimensions of warehouse abuse.

5. Implementation and Methodology

This section describes the technical implementation and methodological approach underlying the proposed **blockchain-integrated warehouse management system (WMS)**. The system is designed using a modular and scalable architecture that supports efficient inventory tracking, automated reconciliation processes, and strengthened cybersecurity measures. The methodology is grounded in data-driven decision-making, leveraging the integration of **IoT**, **AI**, and **blockchain technologies** to enhance operational transparency, mitigate product abuse, and enable the detection of fraudulent activities.

5.1. Implementation

To address complex operational requirements and support large-scale warehouse environments, a **prototype warehouse management system (WMS)** was developed, as depicted in Figure 2. The initial implementation was deployed on **Amazon Web Services (AWS)** using a lightweight technology stack consisting of **PHP, HTML, Bootstrap, and SQLite**, facilitating rapid prototyping and proof-of-concept evaluation.

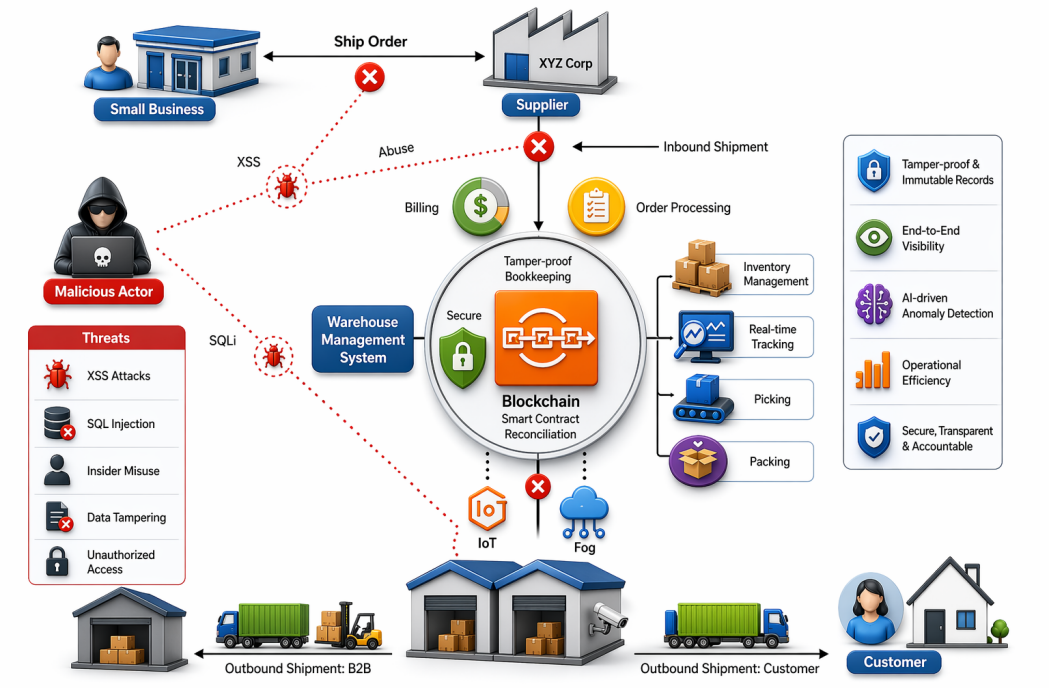

Figure 2. Schematic diagram of an integrated warehouse ecosystem illustrating the interplay between physical assets (warehouses, trucks), inbound and outbound (B2B) shipments, and advanced IT systems (blockchain, IoT tracking, and AI-driven anomaly detection) to streamline operations and mitigate risks posed by potential threat actors.

Following initial validation, the system was restructured to accommodate higher transaction volumes, improved scalability, and seamless integration with advanced analytical components. The enhanced WMS adopts a **service-oriented architecture**, utilizing **Vue.js** for the frontend interface, **Java with Spring Boot** for backend microservices, **Camunda BPM** for workflow orchestration and business process automation, and **PostgreSQL** as the primary data persistence layer.

The finalized system was deployed within a **35,000 sq. ft. warehouse facility**, supporting the processing of over **10 million transactions across a five-year period**. Its modular

architecture enabled integration with IoT sensors and RFID-based tracking systems, while also providing an extensible foundation for future blockchain-based immutable data recording. Core functionalities—including inventory management, billing, order processing, and reconciliation—were implemented as loosely coupled yet interoperable services, communicating through secure RESTful APIs and message queue infrastructures.

Security controls, including encrypted communication protocols (**TLS 1.3**), **token-based authentication mechanisms (JWT)**, and **role-based access control (RBAC)**, were systematically implemented across all system endpoints to ensure secure access and maintain data integrity.

The blockchain layer was **conceptually modeled** as a permissioned consortium network, wherein warehouse operators, suppliers, and logistics providers maintain synchronized ledgers to ensure transparency and non-repudiation of all transactions. Although this component was not physically implemented in the prototype, the proposed architecture illustrates how blockchain integration can support immutable record-keeping, shared accountability, and verifiable auditability among stakeholders in a production environment.

5.2. Data Collection and Optimization

Robust and high-quality data acquisition constitutes a critical foundation of the proposed framework. Information is continuously collected from diverse sources across the warehouse ecosystem to enable effective anomaly detection, enhance process optimization, and improve reconciliation accuracy:

1. **IoT devices** tracking product movement, environmental conditions, and tamper status;
2. **Human operators** contributing manual event inputs and productivity metrics;
3. **Inventory tracking systems** capturing SKU or FNSKU based life cycle events;
4. **Product attributes** such as dimensions, weight, and category;
5. **Operational timestamps** recording task duration and workflow latency;
6. **Receiving and shipment location identifiers** mapping spatial flow of goods; and
7. **External logistics data** including tracking numbers and estimated arrival times from carriers (e.g., FedEx, UPS).

This multidimensional data repository enables the WMS to support both predictive and descriptive analytics for detecting process inefficiencies and identifying potential fraud patterns. Reconciliation accuracy is supported through cross-validation of transactional records across warehouse, customer, and logistics data, while the conceptual blockchain layer illustrates how such records could be maintained immutably in future multi-stakeholder deployments. Any inconsistencies automatically initiate audit procedures and activate AI-driven anomaly detection mechanisms.

The conceptual integration of blockchain would ensure that each recorded event—such as shipment receipt, charge allocation, and delivery confirmation—is **immutable and verifiable**, thereby strengthening trust among stakeholders. Data collected through IoT devices enhances contextual awareness across operations, while AI-based models analyze deviations to distinguish between normal operational variations and potential abuse scenarios. Together, these components form a **closed-loop system** that supports continuous monitoring, risk identification, and ongoing process optimization.

5.3. Methodology

The system development process adopted a **hybrid iterative–incremental approach**, integrating agile prototyping cycles with systematic evaluation of performance and security under simulated operational conditions. The methodology comprised the following phases:

1. **System Design and Modeling:** The system architecture was defined using Camunda BPMN diagrams to model end-to-end workflows, encompassing inbound handling, storage operations, repackaging processes, and outbound reconciliation.
2. **Conceptual Blockchain Integration:** A permissioned blockchain architecture, inspired by Hyperledger Fabric, was conceptually designed to function as a distributed ledger supporting order reconciliation, financial transaction logging, and auditability. Smart contract mechanisms were modeled to automate payment validation and enable conditional release upon verified proof of delivery.
3. **IoT Device Integration:** RFID gateways and heterogeneous sensor infrastructures were configured to capture real-time data on inventory movement, environmental conditions, and shipment telemetry. These data streams enabled analysis of process inefficiencies, latency constraints, and overall operational performance.
4. **AI-Based Anomaly Detection Design:** Supervised machine learning techniques were conceptually developed to detect irregular pricing behaviors, anomalous order patterns, and suspicious access activities. Model parameters were calibrated using synthetic datasets representative of typical warehouse operations.
5. **Testing and Analytical Validation:** System evaluation focused on functional correctness, scalability, and security resilience. The prototype was tested under simulated workloads exceeding twice the expected transaction volume, with performance assessed using metrics such as processing latency, throughput, and reconciliation accuracy to demonstrate conceptual feasibility.

Through this systematic methodology, the study illustrates how a blockchain-enhanced warehouse management system (WMS) can improve accountability, ensure data integrity, and strengthen cybersecurity resilience. The proposed conceptual framework provides a comprehensive roadmap for real-world implementation, demonstrating how the integration of decentralized record-keeping, IoT-derived telemetry, and AI-driven analytics can collectively mitigate product abuse and reinforce trust among supply chain stakeholders.

5.4. Challenges of Implementing Blockchain and Smart Contracts in Warehouse Ecosystems

The proposed blockchain architecture inherently requires multi-stakeholder participation across the supply chain ecosystem, including warehouse operators, suppliers, third-party logistics providers (e.g., UPS, FedEx), and large e-commerce platforms (e.g., Amazon, Walmart). Warehouse accountability challenges span all these actors, and the benefits of blockchain—particularly immutability and decentralized verification—are realized only when all participants contribute to and validate a shared ledger.

However, the practical deployment of such a system, including its smart contract layer, introduces several significant non-technical and operational challenges:

1. **Stakeholder Onboarding Complexity:** A blockchain-based reconciliation framework requires coordinated participation from independent organizations with differing incentives and operational priorities. Encouraging logistics providers, suppliers, and marketplaces to adopt a shared infrastructure presents substantial organizational and economic barriers, making full-scale adoption infeasible within the scope of a single research deployment.
2. **Governance and Ownership Challenges:** A fundamental question in blockchain deployment concerns governance—specifically, which entity or consortium is responsible for maintaining and regulating the network. In a warehouse ecosystem, no single participant can be assumed to act as a universally trusted authority. Establishing a consortium governance model, including policies for node participation, consensus mechanisms, dispute resolution, and data access control, requires cross-organizational agreements that extend beyond the scope of this study.

3. **Smart Contract Standardization and Trust:** The effective use of smart contracts requires all participating entities to agree on shared business logic, including definitions of delivery confirmation, dispute conditions, penalties, and payment triggers. In heterogeneous supply chain environments, these rules vary significantly across stakeholders. Achieving consensus on standardized and legally enforceable smart contract logic introduces additional complexity, as errors or ambiguities in contract design may lead to irreversible financial or operational consequences.
4. **Reusable Transaction Verification Design:** In addition to governance and legal enforceability, smart contract implementation requires maintainable verification logic for related warehouse transaction types. The AdapT package proposed by Górski [65] demonstrates how reusable verification-rule configurations can be applied to smart contracts that process congruous transaction categories. This design principle is relevant to warehouse blockchain applications because inbound receipts, shipment confirmations, discrepancy reports, reconciliation approvals, and payment-release events may share common validation rules while requiring event-specific constraints. Although this study does not implement production smart contracts, the revised framework now identifies reusable verification-rule design as a key requirement for future blockchain-enabled warehouse reconciliation systems.
5. **Deployment Boundary Ambiguity:** Unlike traditional centralized systems, blockchain solutions cannot be meaningfully deployed in isolation within a single warehouse environment. Their effectiveness depends on end-to-end integration across the supply chain, including (i) shipment creation at the supplier, (ii) transit events managed by carriers, (iii) receiving and reconciliation at the warehouse, and (iv) delivery confirmation at the customer endpoint. Without full integration across these stages, the blockchain reduces to a localized append-only log, offering limited advantages over existing audit mechanisms, while smart contracts cannot be reliably triggered due to incomplete event visibility.
6. **Integration with External Systems:** Real-world deployment necessitates deep integration with proprietary systems owned by major stakeholders, such as e-commerce platforms and logistics providers. Due to restricted system access, proprietary constraints, and the absence of standardized interoperability frameworks, such integration is not practically achievable within an academic or single-organization prototype.

Accordingly, both the blockchain infrastructure and its associated smart contract mechanisms are deliberately presented as conceptual and forward-looking extensions of the implemented system, rather than as immediately deployable components.

The implemented WMS already demonstrates:

- A secure and scalable system architecture;
- Enhanced audit logging and reconciliation capabilities;
- Real-world validation over a five-year operational period.

Within this context, the blockchain and smart contract layers are introduced to:

- Address the residual limitations associated with centralized trust models;
- Provide a conceptual blueprint for future consortium-based implementations;
- Illustrate how immutable, cross-organizational auditability and automated reconciliation can be achieved under aligned stakeholder participation.

As noted earlier, the blockchain architecture is modeled as a permissioned consortium network, explicitly acknowledging that such systems require coordinated multi-party participation and cannot be fully validated within a single deployment environment.

6. Results and Discussion

Software vulnerabilities and cybersecurity risks within warehouse management systems (WMS) can lead to significant financial and reputational consequences for both operators and their clients. Incidents such as data breaches, unauthorized access, and system inefficiencies not only erode customer confidence but also increase exposure to legal risks and operational disruptions. In addition, discrepancies in reconciliation across inbound shipments, inventory storage, and outbound deliveries create considerable financial strain, requiring substantial time, labor, and resources to investigate and resolve.

Many warehouse operations follow a commission-based or throughput-oriented model, where profitability is closely tied to the volume of items processed within a given timeframe. Consequently, the implementation of security and reconciliation mechanisms must carefully balance the objective of **fraud and abuse prevention** with the need to maintain high processing efficiency. Overly complex verification and validation procedures can introduce latency, negatively impacting throughput and, in turn, reducing competitiveness and profitability. Therefore, an effective framework must simultaneously ensure **security, transparency, and operational efficiency**.

6.1. System Performance and Operational Efficiency

The developed WMS prototype was deployed in a real-world warehouse environment supporting large-scale operations, including inbound scheduling, inventory storage, repackaging, and outbound processing. Over a five-year period, the system processed more than **10 million transactions** while achieving an uptime exceeding **99.8%**. Even under peak workload conditions, the average API response latency remained below **250 ms**, demonstrating that a modular microservices architecture built with **Spring Boot** and **PostgreSQL** can effectively scale while maintaining low latency and high system reliability.

The integration of the **Camunda BPM** workflow engine enhanced process visibility and coordination across operational units, thereby reducing errors associated with manual task assignment. Logging and auditing mechanisms enabled the identification of critical performance bottlenecks, including queue congestion within labeling and packaging stages. Subsequent workflow optimizations based on these insights resulted in measurable throughput gains of approximately **12–15%**, as evidenced by historical processing time analyses.

6.2. Fraud Detection and Reconciliation Accuracy

The implementation of automated reconciliation functionalities in the enhanced WMS led to a substantial decrease in discrepancies between recorded and actual shipment data. Analysis of historical order variances revealed a **30% reduction** in manual reconciliation requests relative to legacy workflows. These improvements can be attributed to the following factors:

1. Automated matching of purchase orders and received shipments using SKU-based validation;
2. Real-time alerts for missing or duplicated items; and
3. Enhanced dashboards for anomaly reporting and audit traceability.

AI-assisted anomaly detection, assessed during the system design phase, exhibited strong potential to enhance fraud detection accuracy by identifying pricing anomalies and irregular operational patterns. The reported **18–22%** improvement in detection precision was derived from simulation-based evaluation using representative transaction patterns and should be interpreted as a projected outcome rather than a production-validated measurement from the deployed WMS.

6.3. Implementation Journey and Continuous Improvement

The successful deployment of the WMS was driven by an **incremental and adaptive development approach**. Initially developed as a lightweight prototype for a limited user base, the system benefited from tight feedback cycles and rapid iterative improvements. Early-stage evaluations using both synthetic and real operational data enabled the identification of design shortcomings and software defects, thereby preventing their propagation at larger scales.

6.3.1. Early Technical Challenges and Mitigation

A range of software-related challenges were identified and systematically addressed during the implementation process:

- **PHP data type precision errors:** Early software versions utilized integer rather than double precision data types for monetary calculations, causing rounding inconsistencies. This issue was resolved by redefining variable types and conducting test-driven verification across all financial modules.
- **JavaScript rounding discrepancies:** Frontend display values occasionally diverged from backend calculations due to client-side rounding. Centralizing computation on the server ensured consistency across all user interfaces.
- **Database synchronization and maintenance downtime:** Transient data integrity issues emerged during SQLite outages. Migration to PostgreSQL, supplemented by audit tables and manual reconciliation procedures, eliminated these vulnerabilities.

Although full blockchain-based immutability was not implemented, the deployed audit tables offered limited protection against unauthorized modification of records. Nevertheless, these mechanisms lacked the cryptographic guarantees provided by a decentralized ledger, as administrative users still possessed the ability to alter data. This limitation further underscores the necessity of incorporating blockchain-enabled immutability in future system iterations.

6.3.2. Operational Incidents and Organizational Response

During live deployment, the system faced multiple real-world operational challenges, including shipment losses, instances of supplier under-delivery, and occasional pricing discrepancies.

- **Package loss and accountability:** In cases of incomplete deliveries, the installation of **CCTV cameras** at unloading and inspection stations provided verifiable visual evidence. This documentation discouraged internal theft and enabled supplier compensation based on authenticated footage.
- **Accidental losses and misplacement:** Incidents arising from mishandling or misrouting were mitigated through **RFID tracking**, improving traceability and reducing recovery time for misplaced goods.
- **Human error and mispricing:** High employee turnover occasionally led to incorrect shipment plan selection or misapplied service rates. In one documented instance, a pricing misconfiguration caused a **$50,000 overcharge**, later identified during year-end reconciliation and refunded. This incident underscored the necessity of **automated financial modules** to minimize manual dependency.

6.4. Evidence-Based Accountability and Privacy Considerations in Surveillance-Driven Reconciliation

During the early stages of system deployment, a customer reported missing inventory valued at approximately $1000 from a shipment received from a third-party supplier. Due to the absence of verifiable audit mechanisms, the warehouse operator was unable to determine the source of the discrepancy and consequently assumed the financial loss.

Following this incident, CCTV systems were deployed at critical inbound handling points, particularly during box-opening and inspection processes. While similar discrepancy cases continued to occur, the availability of recorded visual evidence enabled accurate identification of the origin of inconsistencies. Consequently, the warehouse was able to reassign financial responsibility to the appropriate party, such as the supplier or logistics provider, thereby eliminating unjustified loss absorption.

This observation highlights that the primary limitation in traditional warehouse operations is not the occurrence of discrepancies but the lack of verifiable and trusted evidence. CCTV-based monitoring provided a practical form of auditability by establishing a visual chain of custody and introducing a deterrence effect against both supplier-side fraud and insider theft.

However, such surveillance mechanisms introduce important privacy and regulatory considerations, particularly in the context of the General Data Protection Regulation (GDPR) and similar data protection frameworks. Continuous video recording may capture personally identifiable information of employees, raising concerns related to lawfulness, proportionality, and data minimization. Furthermore, centralized storage of surveillance data introduces risks associated with unauthorized access, misuse, and extended retention beyond the intended purpose.

To address these concerns, surveillance in the proposed system is conceptually aligned with privacy-preserving design principles, including restricted access to footage, encrypted storage, limited retention periods, and strict purpose limitation (i.e., fraud detection and dispute resolution only). These controls aim to balance operational accountability with employee privacy rights.

Despite its practical benefits, CCTV remains a centralized and potentially mutable form of evidence, lacking standardized mechanisms for cross-organizational verification. This limitation motivates the adoption of blockchain-based approaches. In contrast, a permissioned blockchain architecture enables immutable, tamper-resistant, and shared transaction records across stakeholders, including suppliers, warehouse operators, and logistics providers. By extending auditability from localized visual evidence to cryptographically secured distributed ledgers, blockchain technology supports transparent and trustless reconciliation, reducing dependency on centralized control and mitigating both operational disputes and data integrity risks.

Lessons Learned

Key lessons derived from implementation and operational experience include:

1. **Gradual scaling and iterative refinement**, allowing systematic debugging and controlled feature expansion;
2. **Continuous integration and user feedback**, ensuring usability and alignment with operational workflows;
3. **Strong audit and error detection mechanisms**, compensating for the absence of full blockchain immutability; and
4. **Organizational agility**, reflected in rapid installation of surveillance systems, workforce retraining, and process optimization following early incidents.

The absence of recorded successful cybersecurity incidents leading to data breaches, operational compromise, or unauthorized system access during the five-year observation period supports the effectiveness of the system's secure architecture, well-defined access control mechanisms, and comprehensive API protection strategies.

6.5. Conceptual Blockchain and IoT Enhancements

Although not implemented in the production environment, the **conceptual integration of blockchain and IoT** presented in the system design demonstrates significant potential for enhancing data integrity and auditability in future deployments.

- A **permissioned blockchain ledger** would eliminate administrative tampering and guarantee immutable transaction histories.
- **IoT telemetry and RFID tracking** could enable real-time visibility and environmental monitoring, improving accountability throughout logistics and storage operations.
- **Smart contracts** could automate reconciliation and payment verification, releasing funds only when delivery events are cryptographically validated on-chain.

Simulation-based and analytical estimates suggest that the integration of these technologies could further decrease reconciliation disputes and manual audit requirements by approximately 20–25%, while incurring an estimated performance overhead of around 3–5% per transaction. These values should be interpreted as projected outcomes rather than measurements from the deployed production system.

At the same time, recent HAWS literature emphasizes that prevention and detection strategies are better covered than recovery strategies, while business-continuity planning, backup systems, and back-to-manual protocols remain underexplored for highly automated warehouses [7]. Therefore, the conceptual blockchain and IoT extensions should be interpreted not only as mechanisms for immutability and real-time visibility, but also as components of a broader resilience roadmap that must include redundancy, operational fallback procedures, and recovery validation.

6.6. Financial and Security Impact

From a financial perspective, the deployed WMS yielded quantifiable cost efficiencies by decreasing manual reconciliation efforts and reducing the need for pricing corrections. Internal operational reports indicated an **8–10% reduction** in labor hours associated with reconciliation activities on an annual basis. In addition, overall operational efficiency improved, error rates decreased, and workforce productivity increased as a result of automating previously manual processes.

From a security standpoint, the system's proactive architectural design effectively mitigated risks associated with data breaches, unauthorized access, and insider misuse. During the observed five-year operational period, no recorded successful cybersecurity incidents leading to data breaches, operational compromise, or unauthorized system access were identified through internal monitoring and audit mechanisms. This result can be attributed to a defense-in-depth approach that integrates **TLS encryption, RBAC, MFA**, and **continuous audit logging**. Together, these mechanisms ensured system integrity, safeguarded sensitive information, and strengthened stakeholder trust. Although the system underwent operational security validation through sustained Amazon Marketplace API integration requirements, independent third-party penetration testing was not conducted and remains part of future work.

Table 3 presents a summary of the quantifiable operational and economic benefits realized following the deployment of the proposed WMS integrated with a DSS. The system increased monthly processing capacity from approximately 30,000 to 75,000 items, representing a **150% improvement**, while concurrently reducing reconciliation requests by 40%. Labor hours associated with reconciliation activities declined by 70%, and the average financial impact of reconciliation errors decreased by 85%.

Table 3. Comparative Analysis: Legacy Operations vs. Implemented WMS.

Metric	Before WMS Implementation	After WMS Implementation	Improvement (%)
Average Monthly Throughput (Processed Items)	∼30,000	∼75,000	+150.0
Manual Reconciliation Requests (per Month)	5000	3000	−40.0
Average API Response Latency	520 ms	250 ms	−52.0
Operational Downtime (per Year)	52 h	24 h	−53.8
Reconciliation Labor Hours (per Month)	100 h	30 h	−70.0
Recorded Successful Cybersecurity Incidents	2 minor	0	No successful incidents recorded
Average Mispricing Events (per Year)	30	10	−66.7
Average Cost of Reconciliation Errors	$20,000	$3000	−85.0
Operational Loss	$54,000	$9000	−83.3
Workforce Size	20	35	+75.0
Workforce per 5000 SqFt	5 worker	1 worker	+400.0 efficiency

Importantly, operational throughput increased at a substantially higher rate than workforce growth, indicating that the implemented WMS improved labor productivity and operational scalability rather than introducing workforce inefficiencies.

Additionally, operational downtime was significantly reduced, decreasing from 52 to 24 h per year, and mispricing incidents were lowered by nearly two-thirds. Importantly, no recorded successful cybersecurity incidents were observed following the implementation of integrated auditing and access control mechanisms during the observed operational period.

Although the workforce increased from 20 to 35 employees, this growth reflects operational scaling rather than inefficiency. Productivity per unit area improved significantly, with a single worker now overseeing approximately 5000 sq. ft., compared with five workers required previously. These findings suggest that expansion in operations was accompanied by enhanced automation efficiency and improved operational productivity per processed unit.

Overall, the results indicate that the integrated WMS improved scalability and data transparency while achieving cost efficiency, minimizing downtime, and strengthening overall cybersecurity resilience within warehouse operations.

6.7. Privacy Risks and Insider Threat Scenarios

While performance and security are fundamental to operational effectiveness, **data privacy** constitutes an equally critical aspect of warehouse management [71]. Contemporary WMS platforms aggregate highly sensitive customer and business data, including supplier information, procurement volumes, repackaging activities, and unit pricing for goods distributed through marketplaces such as Amazon. Such data holds significant commercial value, as it can reveal a customer's supply chain strategy, sourcing relationships, and underlying profitability structure.

The privacy and insider-risk concerns discussed in this section are derived from practical observations and governance challenges encountered during long-term warehouse

management system deployment and operation. To preserve customer confidentiality and proprietary business information, illustrative threat scenarios are generalized and abstracted rather than tied to individually identifiable operational incidents.

In this context, **insider-driven data misuse** constitutes a critical privacy and ethical concern. Operational experience demonstrated that unrestricted employee visibility into customer sourcing, pricing, and supplier information introduces significant governance and privacy risks within multi-tenant warehouse ecosystems. Employees or privileged internal users with excessive access to sensitive information could potentially misuse such data for unauthorized competitive or commercial purposes. This form of insider-enabled competition not only erodes customer trust but also introduces significant reputational and legal risks for the warehouse operator.

This risk is further intensified by the fact that identifying profitable products for resale generally demands **significant investment, experimentation, and market analysis**. As a result, WMS data encompasses not only operational logistics but also the outcomes of customers' strategic business experimentation, rendering such information one of the most sensitive and valuable assets within the warehouse ecosystem.

A **privacy preserving WMS architecture** must therefore enforce **strict RBAC** and **context aware data visibility** to safeguard customer information:

- **Role-based screen rendering:** Employees should access only interface components and data relevant to their assigned tasks. For example, packaging personnel should not have visibility into supplier identities or product cost structures.
- **Data segmentation by customer:** Each client's records (including pricing and sourcing data) must be logically isolated at both the database and application layers. Multi-tenant security policies should prevent any form of cross-customer data inference.
- **Auditable access logs:** Every data access or export action must be logged with timestamps, user identifiers, and contextual metadata. Anomalous activity, such as excessive data retrieval or export volume, should automatically trigger alerts.
- **Transparent data ownership:** The WMS provider should maintain and disclose a registry of internal users (e.g., administrators or managers) with elevated access privileges to customer data. Customers should be able to verify whether any of these users operate external e-commerce ventures that could represent conflicts of interest.

From a governance standpoint, the implementation of these safeguards contributes to the establishment of a **mutual trust framework** between warehouse operators and their clients. By enforcing restricted access controls, ensuring traceability, and maintaining transparency in the actions of privileged users, a privacy-preserving WMS prevents the internal misuse of competitive intelligence derived from customer data.

From a conceptual standpoint, incorporating blockchain-based logging can further strengthen this framework by enabling immutable access records, thereby making any instances of insider data misuse both traceable and non-repudiable. Collectively, these mechanisms establish a foundation for **privacy accountability**, ensuring that customers' business-critical information is safeguarded not only against external threats but also against risks stemming from insider-driven competition.

Figure 3 illustrates the privacy-preserving access control framework within the conceptual WMS architecture. Sensitive customer information—such as supplier identities, pricing configurations, and repackaging details—is propagated through the system under strictly controlled conditions, ensuring that each role is granted access only to the data required for its specific functions.

Role-based interface rendering and constrained data access channels limit exposure of confidential business intelligence to operational personnel, while all administrative and audit-related activities are systematically logged to ensure accountability. This approach

prevents insiders from leveraging WMS-acquired data for competitive purposes, thereby maintaining both transparency and trust within the warehouse ecosystem.

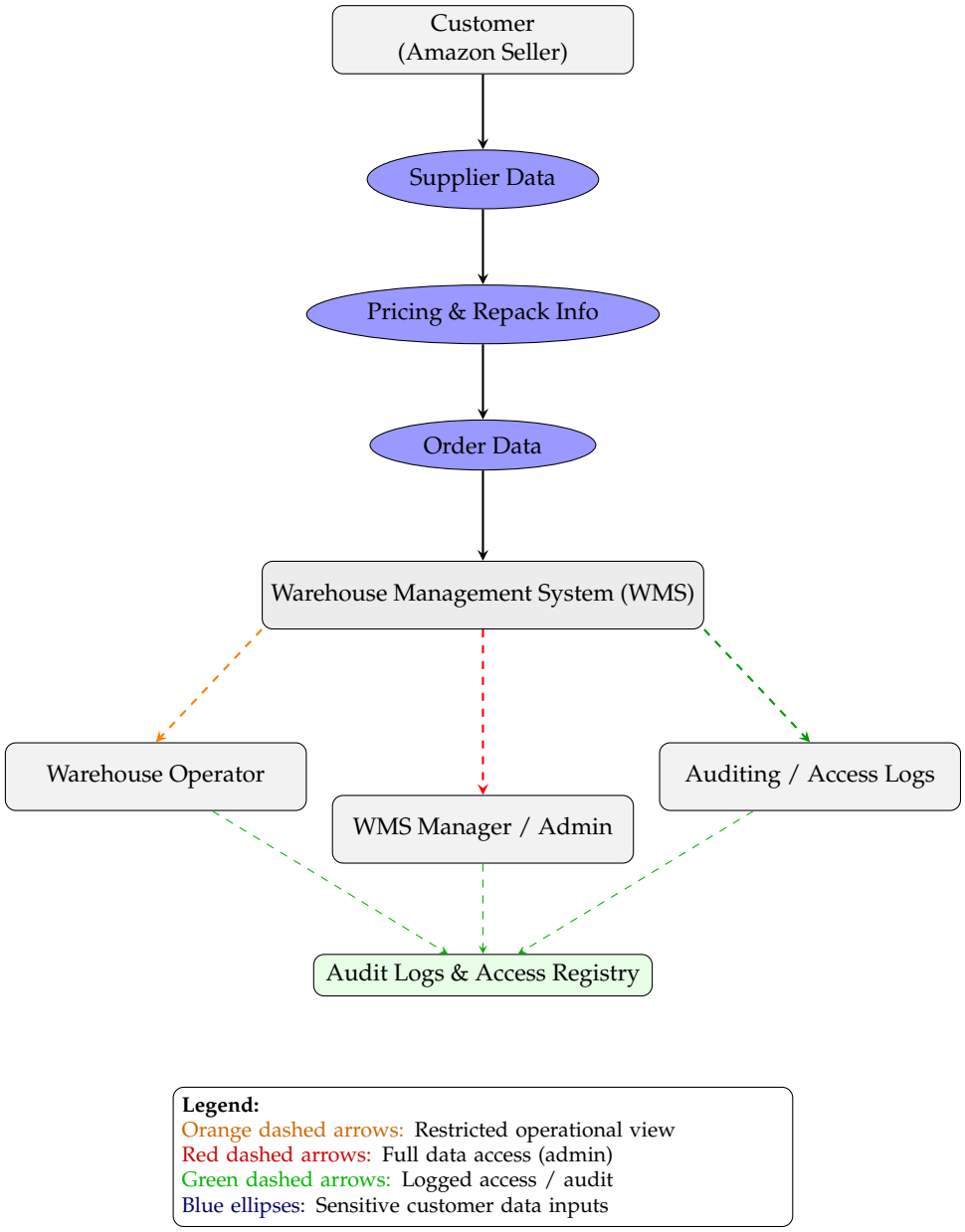

Figure 3. Privacy preserving WMS access control model showing restricted (role-based) data visibility for employees, auditable access registry, and customer data confidentiality enforcement to mitigate insider competition risks [5].

6.8. Discussion

The results indicate that a **progressive, feedback-oriented development strategy** played a central role in the successful deployment and long-term operation of the proposed warehouse management system (WMS). Beginning with a small, testable system core and expanding it iteratively allowed technical issues to be identified early, thereby reducing downstream rework and operational risk. Practical challenges encountered during deployment, including pricing discrepancies, database inconsistencies, shipment losses, and supplier under-delivery, directly informed both software improvements and organizational process changes.

The implemented system demonstrated that a security-conscious WMS can improve operational scalability while reducing reconciliation effort, mispricing events, and opera-

tional losses. The observed improvements in throughput, reconciliation labor, downtime, and error-related costs suggest that automation and structured auditability can produce measurable operational benefits without sacrificing system reliability. In this sense, the study shows that cybersecurity-oriented design should not be viewed as separate from operational efficiency; rather, access control, audit logging, workflow automation, and process visibility can jointly support both performance and accountability.

At the same time, the findings should be interpreted within the boundaries of the implemented system. Although the deployed WMS achieved a high level of operational maturity and exhibited strong security performance during the observed period, several limitations remain. These include reliance on centralized audit tables rather than fully immutable blockchain-based records, the existence of administrative privileges that could theoretically enable data modification, and partial dependence on manual reconciliation for exceptional cases. These limitations indicate that the implemented system represents a secure centralized architecture rather than a fully decentralized trustless ecosystem.

Addressing these limitations would require deeper integration of blockchain, IoT, and AI components. A permissioned blockchain layer could provide stronger guarantees of immutability and non-repudiation for reconciliation and access logs, while IoT- and RFID-based telemetry could improve real-time visibility across inbound, storage, and outbound operations. AI-driven anomaly detection could further strengthen fraud detection by identifying unusual pricing, inventory, access, or shipment patterns. Together, these extensions would enable the transition from a secure centralized WMS toward a more resilient, decentralized, and self-validating warehouse ecosystem.

The broader smart warehouse literature supports this direction. Recent studies on blockchain-enabled warehouse receipts, RFID- and IoT-assisted logistics optimization, digital twins, AR-assisted navigation, voice-driven warehouse interaction, AI-based layout optimization, computer vision, autonomous robots, drones, and robotic process automation collectively show that warehouse systems are evolving toward intelligent, adaptive, and cyber–physical infrastructures [28,35,36,42,44,47,48,64,72,73]. However, much of this literature primarily emphasizes operational efficiency, automation, optimization, and decision support. Comparatively less attention is given to abuse prevention, immutable auditability, insider-risk mitigation, privacy-preserving access control, and cybersecurity-aware reconciliation.

This distinction reinforces the contribution of the present study. Rather than treating security as a secondary technical add-on, the proposed framework positions abuse resistance, traceability, privacy-aware access control, and verifiable accountability as core design objectives of warehouse management systems. The practical deployment demonstrates that these objectives can be integrated with real-world WMS operations, while the conceptual blockchain, IoT, and AI extensions provide a roadmap for strengthening trust and resilience across multi-stakeholder warehouse ecosystems.

These findings should also be interpreted in light of the study limitations discussed below, particularly the single-warehouse evaluation setting, conceptual blockchain layer, and absence of independent third-party penetration testing.

Overall, the findings indicate that the integration of incremental, practice-oriented software engineering with cybersecurity-aware design and organizational adaptability can produce resilient warehouse management solutions that mitigate abuse while maintaining operational efficiency. The study further suggests that future WMS architectures should evolve beyond transactional inventory management toward secure, intelligent, privacy-preserving, and accountable cyber–physical warehouse ecosystems.

6.9. Limitations

Despite the operational improvements and architectural contributions presented in this study, several limitations should be acknowledged. First, the empirical observations and operational evaluations were conducted within a single warehouse environment, which may limit the generalizability of the reported findings across different logistics ecosystems and warehouse scales. Second, portions of the AI-assisted anomaly detection discussion rely on synthetic or simulated datasets due to the limited availability of real-world labeled warehouse cybersecurity incidents. Third, while blockchain-based accountability mechanisms and smart-contract-driven reconciliation workflows were conceptually designed and evaluated from an architectural perspective, a fully operational multi-stakeholder blockchain deployment was not implemented because of onboarding, interoperability, governance, and ecosystem coordination challenges among external logistics and supply chain participants. Finally, although the warehouse system demonstrated strong operational resilience during the observation period, the cybersecurity evaluation did not include independent third-party penetration testing or external security audits. Future research should focus on multi-site validation, real-world IIoT attack datasets, blockchain interoperability experimentation, and longitudinal warehouse cybersecurity benchmarking across larger supply chain ecosystems.

7. Conclusion and Future Work

This study presented the design and implementation of a **warehouse management system (WMS)** aimed at mitigating product abuse, privacy risks, and fraudulent activities within warehouse operations. The system was deployed in a 35,000 sq. ft. production environment and demonstrated measurable improvements in process efficiency, reconciliation accuracy, and operational transparency. Over a five-year operational period, the platform successfully processed more than **10 million transactions** without any recorded successful cybersecurity incidents leading to data breaches, operational compromise, or unauthorized system access, underscoring the robustness of its architectural design and access control mechanisms.

The **proposed blockchain-enhanced framework**, while conceptually developed rather than fully implemented, extends the capabilities of the deployed system by incorporating immutable transaction logging, AI-based fraud detection, and smart contract-driven reconciliation. Collectively, these components define a pathway toward a secure and abuse-resilient warehouse ecosystem. Blockchain technology enables tamper-resistant auditability, AI techniques improve anomaly detection, and smart contracts facilitate automated accountability among stakeholders. This integrated approach enhances both security and privacy while establishing verifiable trust and financial transparency across customers, suppliers, and logistics providers.

The effectiveness of the WMS implementation can be attributed to its **incremental development approach** and continuous improvement cycle. Initial deployment with a limited customer base enabled rapid detection and resolution of issues, including data type inconsistencies in PHP, rounding errors in JavaScript, and database anomalies. Real-world operational events—such as shipment losses, supplier under-deliveries, and pricing inaccuracies—served as key drivers for iterative system enhancements.

The adoption of measures such as CCTV monitoring, RFID-based tracking, and automated pricing mechanisms significantly reduced loss incidents and minimized human error. These findings underscore the importance of progressive system scaling, continuous stakeholder feedback, and proactive error management in the development of secure, enterprise-grade solutions.

From a security standpoint, the use of audit tables and layered access control mechanisms provided an initial level of data integrity protection; however, these measures do not offer the same guarantees as blockchain-based immutable ledgers. The conceptual evaluation indicates that integrating blockchain technology would significantly enhance auditability and eliminate the risk of administrative data manipulation, enabling the evolution of the WMS from a secure centralized system into a decentralized, trustless infrastructure appropriate for consortium-based warehouse operations.

Future extensions of this research should explore the following directions:

- **Federated AI Models for Warehouse Anomaly Detection:** Enabling multiple warehouses to collaboratively train fraud detection and performance optimization models without exposing sensitive customer or supplier data.
- **Tokenized Digital Identity for Warehouse Personnel:** Developing cryptographically verifiable identity systems to immutably record all employee actions on blockchain, thereby reducing insider threats and enhancing accountability.
- **Decentralized Supply Chain Consortiums:** Extending the architecture to a permissioned, multiwarehouse blockchain network in which customers, suppliers, and logistics providers share a unified ledger to improve traceability and reduce shipment fraud.
- **Privacy Preserving WMS Architecture:** Integrating role-based screen rendering, granular access control, and immutable access logs to prevent insider misuse of sensitive customer or supplier data.
- **Scalability and Interoperability Studies:** Evaluating performance trade-offs, transaction throughput, and seamless integration of blockchain modules with existing enterprise WMS and ERP platforms.
- **Resilience and Recovery Planning for Highly Automated Warehouses:** Developing and empirically testing backup systems, supplier-swapping strategies, recovery-time objectives, and back-to-manual operating procedures for WMS-dependent and IoT-enabled warehouse environments, responding to the documented research gap in HAWS recovery capabilities [7].

Future research should additionally evaluate the proposed framework across multiple warehouse operators, geographic regions, and supply chain domains to improve external validity and comparative benchmarking.

In conclusion, this study demonstrates that a **security-centric WMS design**, when integrated with data integrity mechanisms, privacy-preserving controls, and conceptual blockchain components, can substantially improve accountability and trust within warehouse logistics. The implemented system confirms the practical feasibility and advantages of this approach, while the proposed conceptual extensions provide a viable roadmap for the development of large-scale, distributed, and tamper-resistant warehouse ecosystems in future deployments.

Author Contributions: Conceptualization, A.S. and I.B.; methodology, A.S. and I.B.; software, A.S.; validation, A.S.; formal analysis, A.S.; investigation, A.S.; resources, A.S.; data curation, A.S.; writing—original draft preparation, A.S. and I.B.; writing—review and editing, A.S. and I.B.; visualization, A.S.; supervision, I.B.; project administration, I.B.; funding acquisition, not applicable. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data supporting the findings of this study are not publicly available due to customer privacy, confidentiality, and proprietary business restrictions. The study is based on operational warehouse records involving real customer transactions, supplier information, shipment details, and internal system logs. Aggregated and anonymized results are presented in the manuscript;

however, the underlying raw data cannot be shared because disclosure could compromise customer confidentiality and commercially sensitive operational information.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this study:

3PL	Third-Party Logistics
ABAC	Attribute-Based Access Control
AGV	Automated Guided Vehicle
AI	Artificial Intelligence
AMR	Autonomous Mobile Robot
API	Application Programming Interface
AR	Augmented Reality
AS/RS	Automated Storage and Retrieval System
AWS	Amazon Web Services
B2B	Business-to-Business
BPMN	Business Process Model and Notation
CCTV	Closed-Circuit Television
CSP	Content Security Policy
DB	Database
DDoS	Distributed Denial of Service
DLP	Data Loss Prevention
DSS	Decision Support System
ERP	Enterprise Resource Planning
FNSKU	Fulfillment Network Stock Keeping Unit
GDPR	General Data Protection Regulation
G2P	Goods-to-Person
HAWS	Highly Automated Warehouse Systems
HTML	HyperText Markup Language
HTTPS	HyperText Transfer Protocol Secure
IoT	Internet of Things
IIoT	Industrial Internet of Things
IT	Information Technology
JSON	JavaScript Object Notation
JWT	JSON Web Token
LLM	Large Language Model
MITM	Man-in-the-Middle
ML	Machine Learning
MFA	Multi-Factor Authentication
mTLS	Mutual Transport Layer Security
OAuth	Open Authorization
PHP	PHP: Hypertext Preprocessor
PoD	Proof of Delivery
PWA	Progressive Web Application
RBAC	Role-Based Access Control
REST	Representational State Transfer
RFID	Radio Frequency Identification
RTLS	Real-Time Location System
SDLC	Software Development Lifecycle
SKU	Stock Keeping Unit
SQL	Structured Query Language
SQLi	SQL Injection

TLS	Transport Layer Security
WAF	Web Application Firewall
WCS	Warehouse Control System
WMS	Warehouse Management System
XSS	Cross-Site Scripting
ZTA	Zero Trust Architecture

References

1. Sari, A.; Butun, I. A Case Study of Decision Support System and Warehouse Management System Integration. In *Decision Support Systems and Industrial IoT in Smart Grid, Factories, and Cities*; IGI Global: Hershey, PA, USA, 2021; pp. 111–138.
2. Sari, A.; Lekidis, A.; Butun, I., Industrial Networks and IIoT: Now and Future Trends. In *Industrial IoT: Challenges, Design Principles, Applications, and Security*; Springer International Publishing: Cham, Switzerland, 2020; pp. 3–55. [CrossRef]
3. Lin, H.; Li, X.; Liu, F. Multi-warehouse assortment selection: Minimizing order splitting in e-commerce logistics. *Prod. Oper. Manag.* **2026**, *35*, 1074–1094. [CrossRef]
4. Sari, A.; Butun, I. Blockchain-Enhanced Warehouse Management: Mitigating Product Abuse and Privacy Risks. In *Proceedings of the 2025 International Conference on Smart Applications, Communications and Networking (SmartNets)*; IEEE: Piscataway, NJ, USA, 2025; pp. 1–6.
5. Sari, A. Mitigating Product Abuse Through Privacy-Preserving and Secure Technologies in Digital and Industrial Systems. Ph.D. Thesis, University of Delaware, Newark, DE, USA, 2025.
6. Butun, I. Privacy and trust relations in internet of things from the user point of view. In *Proceedings of the 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*; IEEE: Piscataway, NJ, USA, 2017; pp. 1–5.
7. Rodríguez-García, M.; Kembro, J.H.; Betts, K.; Ponce-Cueto, E. Managing technology-related disruptions and vulnerabilities in highly automated warehouse systems: An integrative review and research agenda. *Int. J. Prod. Res.* **2026**, *64*, 1676–1708. [CrossRef]
8. Marziali, M.; Rossit, D.A.; Toncovich, A. Warehouse management problem and a kpi approach: A case study. *Manag. Prod. Eng. Rev.* **2021**, *12*, 51–62. [CrossRef]
9. Torabizadeh, M.; Yusof, N.M.; Ma'aram, A.; Shaharoun, A.M. Identifying sustainable warehouse management system indicators and proposing new weighting method. *J. Clean. Prod.* **2020**, *248*, 119190. [CrossRef]
10. Andiyappillai, N. Factors influencing the successful implementation of the warehouse management system (WMS). *Int. J. Comput. Appl.* **2020**, *177*, 21–25. [CrossRef]
11. Mostafa, N.; Hamdy, W.; Elawady, H. An intelligent warehouse management system using the internet of things. *Egypt. Int. J. Eng. Sci. Technol.* **2020**, *32*, 59–65. [CrossRef]
12. Amanda Istiqomah, N.; Fara Sansabilla, P.; Himawan, D.; Rifni, M. The implementation of barcode on warehouse management system for warehouse efficiency. *J. Phys. Conf. Ser.* **2020**, *1573*, 012038. [CrossRef]
13. Halawa, F.; Dauod, H.; Lee, I.G.; Li, Y.; Yoon, S.W.; Chung, S.H. Introduction of a real time location system to enhance the warehouse safety and operational efficiency. *Int. J. Prod. Econ.* **2020**, *224*, 107541. [CrossRef]
14. Lee, C.K.; Lv, Y.; Ng, K.K.; Ho, W.; Choy, K.L. Design and application of Internet of things-based warehouse management system for smart logistics. *Int. J. Prod. Res.* **2018**, *56*, 2753–2768. [CrossRef]
15. Čolaković, A.; Čaušević, S.; Kosovac, A.; Muharemović, E. A review of enabling technologies and solutions for IoT based smart warehouse monitoring system. In *Proceedings of the International Conference "New Technologies, Development and Applications"*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 630–637.
16. Li, S.; You, X.; Sun, Z. Drug Management System Based on RFID. In *Data Processing Techniques and Applications for Cyber-Physical Systems (DPTA 2019)*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 1955–1958.
17. Dhaliwal, A. The rise of automation and robotics in warehouse management. In *Transforming Management Using Artificial Intelligence Techniques*; CRC Press: Boca Raton, FL, USA, 2020; pp. 63–72.
18. Kordos, M.; Boryczko, J.; Blachnik, M.; Golak, S. Optimization of warehouse operations with genetic algorithms. *Appl. Sci.* **2020**, *10*, 4817. [CrossRef]
19. Bottani, E.; Casella, G.; Monferdini, L. Tracing the evolution of warehouse technologies: A bibliometric study. *Procedia Comput. Sci.* **2025**, *253*, 2951–2960. [CrossRef]
20. Tiwari, S. Smart warehouse: A bibliometric analysis and future research direction. *Sustain. Manuf. Serv. Econ.* **2023**, *2*, 100014. [CrossRef]
21. Purnomo, L. Offline-First Warehouse Management for Remote Mining: A Progressive Web Application Deployment in East Kalimantan. Available online: https://ssrn.com/abstract=6346365 (accessed on 15 May 2026).

22. Priyambodo, A.K.; Alzami, F.; Nurhindarto, A.; Winarno, A.; Erawan, L.; Suharnawi, S.; Sulistyono, M.T. Compliance-by-Design for Bonded Warehouses: A Web-Based Inventory System with CEISA-Verified Gate Control and D&M Success Evaluation. *Sink. J. Dan Penelit. Tek. Inform.* **2026**, *10*, 741–754.
23. Ekren, B.Y.; Venkatadri, U.; Sgarbossa, F.; Grosse, E.H. Warehousing 5.0 for the future of the logistics industry. *Int. J. Prod. Res.* **2026**, *64*, 1587–1597. [CrossRef]
24. Nicoletti, B.; Appolloni, A. Green Warehouse 5.0. In *The Future of Industry: Human-Centric Approaches in Digital Transformation*; Springer: Berlin/Heidelberg, Germany, 2024; pp. 303–320.
25. Delfanti, A. *The Warehouse: Workers and Robots at Amazon*; Pluto Books: London, UK, 2021.
26. Kembro, J.H.; Norrman, A. A strategic perspective on automated warehouse systems in retail: insights from a multiple case study. *Int. J. Phys. Distrib. Logist. Manag.* **2025**, *55*, 57–91. [CrossRef]
27. Elbouzidi, A.D.; Frédéric, R.; Pellerin, R.; Lamouri, S.; Ait El Cadi, A. Leveraging digital twins for enhanced sustainable warehouse management. *Clean. Logist. Supply Chain.* **2025**, *17*, 100287. [CrossRef]
28. Rizqi, Z.U.; Chou, S.Y.; Cahyo, W.N. A simulation-based Digital Twin for smart warehouse: Towards standardization. *Decis. Anal. J.* **2024**, *12*, 100509. [CrossRef]
29. Marah, H.; Challenger, M. Madtwin: A framework for multi-agent digital twin development: Smart warehouse case study. *Ann. Math. Artif. Intell.* **2024**, *92*, 975–1005. [CrossRef]
30. Drissi Elbouzidi, A.; Ait El Cadi, A.; Pellerin, R.; Lamouri, S.; Tobon Valencia, E.; Bélanger, M.J. The role of AI in warehouse digital twins: Literature review. *Appl. Sci.* **2023**, *13*, 6746. [CrossRef]
31. Traore, A.; Hervet, É.; Couturier, A. Smolrgpt: Efficient spatial reasoning for warehouse environments with 600m parameters. In Proceedings of the IEEE/CVF International Conference on Computer Vision, Honolulu, HI, USA, 19–20 October 2025; pp. 5271–5279.
32. De Assis, R.F.; Faria, A.F.; Thomasset-Laperrière, V.; Santa-Eulalia, L.A.; Ouhimmou, M.; de Paula Ferreira, W. Machine learning in warehouse management: A survey. *Procedia Comput. Sci.* **2024**, *232*, 2790–2799. [CrossRef]
33. Sodiya, E.O.; Umoga, U.J.; Amoo, O.O.; Atadoga, A. AI-driven warehouse automation: A comprehensive review of systems. *GSC Adv. Res. Rev.* **2024**, *18*, 272–282. [CrossRef]
34. Hernández, C.; López, M.; García, J.; Vander Peterson, C. Optimizing collaborative intelligence systems for end-to-end cybersecurity monitoring in global supply chain networks. *Int. J. Responsible Artif. Intell* **2024**, 28–36.
35. Hořejší, P.; Macháč, T.; Šimon, M. Reliability and accuracy of indoor warehouse navigation using augmented reality. *IEEE Access* **2024**, *12*, 94506–94519. [CrossRef]
36. Song, X. Optimizing the human-computer interaction interface of warehouse management systems using automatic speech recognition technology. In *Proceedings of the 2024 4th International Conference on Computer Science, Electronic Information Engineering and Intelligent Control Technology (CEI)*; IEEE: Piscataway, NJ, USA, 2024; pp. 461–464.
37. Ieva, S.; Bilenchi, I.; Gramegna, F.; Pinto, A.; Scioscia, F.; Ruta, M.; Loseto, G. Enhancing last-mile logistics: AI-driven fleet optimization, mixed reality, and large language model assistants for warehouse operations. *Sensors* **2025**, *25*, 2696. [CrossRef]
38. Berlec, T.; Corn, M.; Varljen, S.; Podržaj, P. Exploring Decentralized Warehouse Management Using Large Language Models: A Proof of Concept. *Appl. Sci.* **2025**, *15*, 5734. [CrossRef]
39. Tan, S.J.; Ong, L.Y.; Leow, M.C. A Systematic Review On Automated Warehouse With Multiple-Deep Rack. *IEEE Access* **2025**, *13*, 40103–40114. [CrossRef]
40. Rad, F.; Oghazi, P.; Onur, İ.; Kordestani, A. Adoption of AI-based order picking in warehouse: Benefits, challenges, and critical success factors. *Rev. Manag. Sci.* **2025**, *19*, 3495–3540. [CrossRef]
41. Daios, A.; Xanthopoulos, A.; Folinas, D.; Kostavelis, I. Towards automating stocktaking in warehouses: Challenges, trends, and reliable approaches. *Procedia Comput. Sci.* **2024**, *232*, 1437–1445. [CrossRef]
42. Shahroudnejad, A.; Mousavi, P.; Perepelytsia, O.; Sahir.; Staszak, D.; Taylor, M.E.; Bawel, B. A novel framework for automated warehouse layout generation. *Front. Artif. Intell.* **2024**, *7*, 1465186. [CrossRef]
43. Tufano, A.; Accorsi, R.; Manzini, R. A machine learning approach for predictive warehouse design. *Int. J. Adv. Manuf. Technol.* **2022**, *119*, 2369–2392. [CrossRef]
44. Keith, R.; La, H.M. Review of autonomous mobile robots for the warehouse environment. *arXiv* **2024**, arXiv:2406.08333. [CrossRef]
45. Li, K.; Liu, L.; Chen, J.; Yu, D.; Zhou, X.; Li, M.; Wang, C.; Li, Z. Research on reinforcement learning based warehouse robot navigation algorithm in complex warehouse layout. In *Proceedings of the 2024 6th International Conference on Artificial Intelligence and Computer Applications (ICAICA)*; IEEE: Piscataway, NJ, USA, 2024; pp. 296–301.
46. Wu, S.; Fu, L.; Chang, R.; Wei, Y.; Zhang, Y.; Wang, Z.; Liu, L.; Zhao, H.; Li, K. Warehouse robot task scheduling based on reinforcement learning to maximize operational efficiency. *Authorea Prepr.* **2025** .
47. Ali, S.S.; Khan, S.; Fatma, N.; Ozel, C.; Hussain, A. Utilisation of drones in achieving various applications in smart warehouse management. *Benchmarking Int. J.* **2024**, *31*, 920–954. [CrossRef]

48. Vu, V.D.; Hoang, D.D.; Tan, P.X.; Nguyen, V.T.; Nguyen, T.U.; Hoang, N.A.; Phan, K.T.; Tran, D.T.; Vu, D.Q.; Ngo, P.Q.; et al. Occlusion-robust pallet pose estimation for warehouse automation. *IEEE Access* **2024**, *12*, 1927–1942. [CrossRef]
49. Krnjaic, A.; Steleac, R.D.; Thomas, J.D.; Papoudakis, G.; Schäfer, L.; To, A.W.K.; Lao, K.H.; Cubuktepe, M.; Haley, M.; Börsting, P.; et al. Scalable multi-agent reinforcement learning for warehouse logistics with robotic and human co-workers. In *Proceedings of the 2024 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*; IEEE: Piscataway, NJ, USA, 2024; pp. 677–684.
50. Qin, H.; Xiao, J.; Ge, D.; Xin, L.; Gao, J.; He, S.; Hu, H.; Carlsson, J.G. JD. com: Operations research algorithms drive intelligent warehouse robots to work. *INFORMS J. Appl. Anal.* **2022**, *52*, 42–55.
51. Minashkina, D. A review and research agenda for recent socially and environmentally sustainable practices for warehouse management systems. *Int. J. Logist. Manag.* **2024**, *35*, 60–98. [CrossRef]
52. Minashkina, D.; Happonen, A. Warehouse management systems for social and environmental sustainability: A systematic literature review and bibliometric analysis. *Logistics* **2023**, *7*, 40. [CrossRef]
53. Li, H.; Wang, S.; Zhen, L.; Wang, X. Data-driven optimization for automated warehouse operations decarbonization. *Ann. Oper. Res.* **2024**, *343*, 1129–1156. [CrossRef]
54. Rahman, M.A.; Kirby, E.D. The Lean advantage: Transforming e-commerce warehouse operations for competitive success. *Logistics* **2024**, *8*, 129. [CrossRef]
55. De Jesus Pacheco, D.A.; Clausen, D.M.; Bumann, J. A multi-method approach for reducing operational wastes in distribution warehouses. *Int. J. Prod. Econ.* **2023**, *256*, 108705. [CrossRef]
56. Živičnjak, M.; Rogić, K.; Bajor, I. Case-study analysis of warehouse process optimization. *Transp. Res. Procedia* **2022**, *64*, 215–223. [CrossRef]
57. Saderova, J.; Rosova, A.; Behunova, A.; Behun, M.; Sofranko, M.; Khouri, S. Case study: The simulation modelling of selected activity in a warehouse operation. *Wirel. Netw.* **2022**, *28*, 431–440. [CrossRef]
58. de Oliveira, A.V.; Pimentel, C.M.O.; Godina, R.; Matias, J.C.d.O.; Garrido, S.M.P. Improvement of the Logistics Flows in the Receiving Process of a Warehouse. *Logistics* **2022**, *6*, 22. [CrossRef]
59. Voronova, O. Improvement of warehouse logistics based on the introduction of lean manufacturing principles. *Transp. Res. Procedia* **2022**, *63*, 919–928. [CrossRef]
60. Fauzan, R.; Shiddiq, M.; Raddlya, N. The designing of warehouse management information system. *IOP Conf. Ser. Mater. Sci. Eng.* **2020**, *879*, 012054. [CrossRef]
61. Zhang, Y.; Pan, F. Design and implementation of a new intelligent warehouse management system based on MySQL database technology. *Informatica* **2022**, *46*, 355–364. [CrossRef]
62. Shanmugamani, K.; Mohamad, F. The implementation of warehouse management system (wms) to improve warehouse performance in business to business (B2B). *Int. J. Ind. Manag.* **2023**, *17*, 231–239. [CrossRef]
63. Serafino, R. Systematic Literature Review: Cold Store Warehouse Management System Implementation in the Western Cape Fruit Sector. Available online: https://ssrn.com/abstract=6391570 (accessed on 15 May 2026).
64. Chen, Y.; Ou, W.; Pang, M.; Ma, J.; Yue, Q.; Han, W. A cross-chain model for warehouse receipts in port supply chain based on notary mechanism and ShangMi cryptographic algorithms. *Sci. Rep.* **2025**, *15*, 14390. [CrossRef]
65. Górski, T. AdapT: A reusable package for implementing smart contracts that process transactions of congruous types. *Softw. Impacts* **2024**, *21*, 100694. [CrossRef]
66. Butun, I.; Sari, A.; Österberg, P. Security Implications of Fog Computing on the Internet of Things. In Proceedings of the 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 11–13 January 2019; pp. 1–6. [CrossRef]
67. I. Butun, A. Sari, and P. Österberg. Hardware security of fog end-devices for the internet of things. *Sensors* **2020**, *20*, 5729. [CrossRef]
68. Butun, I.; Sari, A. Early Detection and Recovery Measures for Smart Grid Cyber-Resilience. In *Decision Support Systems and Industrial IoT in Smart Grid, Factories, and Cities*; IGI Global: Hershey, PA, USA, 2021; pp. 91–110.
69. Rajendiran, G.R. Distributed Ledger Technology for Transparent and Secure Warehouse Inventory Tracking. *J. Curr. Sci. Res. Rev.* **2025**, *3*, 1 –10.
70. Rose, S.; Borchert, O.; Mitchell, S.; Connelly, S. Zero trust architecture. *NIST Spec. Publ.* **2020**, *800*, 1–52.
71. Gaba, G.S.; Sari, A.; Butun, I.; Singh, P.; Gurtov, A.; Liyanage, M. A Survey on Security and Privacy of Industry 4.0 and Beyond: Technical Aspects, Use Cases, Challenges, and Research Directions. *IEEE Open J. Commun. Soc.* **2025**, *6*, 8865–8929. [CrossRef]
72. Fidlerova, H.; Kuka, M.; Adamczak, M. Innovative solutions for warehouse logistics: Improving efficiency with RFID and IoT integration. *Acta Logist.* **2025**, *12*, 137–145. [CrossRef]
73. Nalgozhina, N.; Uskenbayeva, R. Automating hybrid business processes with RPA: Optimizing warehouse management. *Procedia Comput. Sci.* **2024**, *231*, 391–396. [CrossRef]