Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Cybersecurity Risk Management and Zero Trust Transformation in Retail and Supply Chain Sectors

Prassanna Rao Rajgopal
Cybersecurity Leader, Member IEEE & ISACA Raleigh, North Carolina, USA ORCID: 0009-0009-7461-5220
Email: prassannarr@gmail.com

ARTICLE INFO

Received: 09 Oct 2025
Revised: 03 Nov 2025
Accepted: 18 Nov 2025

ABSTRACT

The retail and global supply chain becomes more vulnerable to cyber risks like never before, with the increased pace of digitalization coupled with omni-channel stores, dispersed inventories, payment establishments, vendor-related systems, and cloud-based commerce architecture. The traditional perimeter-based security models now fail to prevent such advanced cyber threats as credential compromise, ransomware attacks, and infiltrations into the supply chain. Threat actors are taking advantage of identity trust problems, third-party integrations, a lack of network segmentation, and limited visibility on both OT and IT networks as the retail businesses embrace cloud services, IoT sensors, POS terminals, e-commerce platforms, robotics, and automation in the warehouse. Zero Trust has taken root as a structure that removes implicit trust and mandates continuous user, equipment, workload, and data stream monitoring in hybrid retail environments. The current paper examines the practices of cybersecurity risk management and assesses the implementation of Zero Trust in the Supply Chain and retail companies. Our offered architecture draws on identity-based access control, micro-segmentation, device attestation, API-level security, data management, and policy enforcement of an automated nature. We also suggest a risk corresponding security lifecycle, the continuous detection, the fusion of threat intelligence, the prioritization of vulnerabilities, the verification of the supply chain, and the identification of anomalies with the help of AI. An actual case study example proves quantifiable positive changes in threat containment, resilience, and operational continuity following the implementation of Zero Trust in a large international retail company. Findings emphasize the use of Zero Trust as a powerful defensive model that can help contemporary retailers reduce cyber risk and safeguard sensitive customer and transaction data, build secure inventory and logistics, and maintain regulatory compliance. The research is summarized with strategic models of organizations that may implement Zero Trust, such as identity modernization, resilience automation, and ongoing risk measurement in the retail value chain.

Keywords: Zero Trust Architecture (ZTA), retail cybersecurity, supply chain security, risk governance, OT/IT convergence, identity access management, micro-segmentation, XDR/SOAR, Zero Trust Network Access (ZTNA), cloud security.

INTRODUCTION

Increasingly rapid omni-channel commerce, real-time inventory visibility, warehouse robotics, cloud adoption, and AI-enabled logistics are transforming retail and supply chain ecosystems at an accelerated pace. As businesses upgrade their archaic ERP systems and monolithic trading systems to microservice-based API-based enterprises and cloud-native systems, the economic surface of the cyber-attack grows exponentially. Some of the threats to retailers now include insiders misusing their credit cards and accessing and exploiting their networks, ransomware on a large scale, backdoor attacks of supply chains, and point-of-sale attacks, as well as stealing the credentials of retailers.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Contemporary retail businesses have incorporated electronic point of sale (POS) systems, warehouse management systems (WMS), ERP systems, IoT sensors, handheld scanning devices, RFID tracking, automation of delivery, and third-party logistics (3PL) networks. This combination is more and more powerful to make speed and customer experience, as well as to provide adversaries with a chance to move laterally. These environments are not appropriately secured using traditional perimeter controls, VPN controlled access, and trust-by-default authentication models. The definition of Zero Trust done by NIST SP 800-207 offers a holistic solution revolving around least-privilege access, identity authentication, a health attestation of devices, and ongoing trust assessment. In the case of retail organizations, Zero Trust represents a necessity and enhancement of security, not only to keep the business running but also to gather and preserve customer, intellectual property, and customer information, as well as preserve the continuity of the logistics and distribution chain.

This study assesses cybersecurity issues in retail and presents a strategy of cybersecurity risk management in the form of a Zero Trust. It suggests a reference model of retail and supply chain settings and provides a real-life implementation example that shows security, resiliency, and operational worth. The purpose of the paper is to give the retailers and supply-chain operators practical advice on the way to a Zero Trust future that ensures revenue, customer trust, and operational integrity are not compromised. The article is organized in such a way that the main cybersecurity issues in the retail and supply chain are introduced in the first place. Section 2 offers a background of these hurdles, such as the role of digital transformation and the multidimensionality of cybersecurity risk management. Section 3 provides the introduction to Zero Trust and the main elements of it, and its application in the context of retail and supply chain. Section 4 is the research methodology; how the research will be conducted and how data and information will be gathered and analysed. Section 5 provides a reference architecture for applying a Zero Trust, whereas Section 6 gives an extensive cybersecurity risk management framework. Section 7 presents a real-life example of the implementation of Zero Trust in a retail company and illustrates how Zero Trust affects both security and the continuity of operations. Lastly, Section 8 will provide results analysis, which will correspond to the quantifiable impact of Zero Trust implementation and the obstacles organizations encounter on the way to it. Section 9 of the paper summarizes strategic advice that retailers implement Zero Trust, encompassing important lessons and future trends.

2. BACKGROUND AND CHALLENGES

There is a radical digital shift in the retail and supply chain industry, and its key advantages and unique cybersecurity threats are present. This is a discussion of the relevant issues that have contributed to complexity of cybersecurity in the discussed industries which include technological innovations, operational issues and development of cyber threats. The background issues provide an explanation of why the previous perimeter-driven security models no longer work, and why Zero Trust is emerging as a crucial solution.

2.1 Digital Revolution and Scale of the Cyberattack.

With the development of Omni channel commerce, the use of cloud computing, and the use of warehousing automation, as well as mobility platforms, the digital transformation of the retail and supply chain ecosystems has been immense [1]. The advances have caused operation efficiency, enhanced customer experiences, and data analytics. However, the retailers, too, have been subjected to the emergence of new threats associated with the rise of the digital service market which compared to the amount of a cyberattack to the emergence of a massive digital surface [2]. The retail operation, as compared to the centralized IT systems, operates across geographically fragmented units like stores, fulfillment center, logistics node, and enormous partner systems, which establish a networked and fragmented technology footprint. Cyber adversaries can exploit vulnerabilities of the endpoints, which can be the POS terminals, barcode readers, IoT devices, and e-commerce APIs.In addition, old operational technology (OT) systems and point-of-sale (POS) systems at the stores were not updated and may not have been modernised to have security features, which remain a persistent vulnerability.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The increased attack surface that is created when retail organizations bring automation and IoT devices into their operations is an unwelcome discovery that exposes the critical systems that these organizations use to opportunistic and highly advanced cyber adversaries. These environments are difficult to provide with a sufficient level of security due to insecure communication channels, out-of-date firmware, and ineffective authentication mechanisms that involve thousands of interconnected devices.

Figure 1 illustrate, the digital transformation within retail and supply chain ecosystems has significantly expanded the cyberattack surface, creating new vulnerabilities in the networked technology footprint, including POS terminals, IoT devices, and e-commerce APIs

Figure 1: E-Commerce Readiness

2.2 Identity and Access Management Problems.

The complexity of identity and access management (IAM) is considered to be a key barrier to retailers in curbing the risk of cybersecurity. The retailing system is characterized by a high level of staff turnover, seasonal employee increase, and temporary hiring of staff, especially at peak times like the periods during holidays. Also, retailers have to host contractors, last-mile delivery workers, and supplier representatives, and each of them needs different access to the system. Such dynamic trends in the workforce make it difficult to manage the credential lifecycles, and frequently result in credential reuse, shared logins, incomplete de-provisioning, and inconsistent application of authentication policy.

Consequently, identity-based attacks (credential theft, phishing, and privilege escalation) are an issue that is common throughout the industry. Attackers are taking the opportunity of such compromised identities to cross-system godfather with weakly managed systems, as well as pointing out the inefficiency of past access control systems like static passwords and role-based access controls (RBAC) without contextual risk scoring. Besides, VPN-based trust models which assume that once a user is verified, they are trusted and authorized to access are no longer applicable in modern distributed environments. The increased relevance of identity as the new perimeter necessitates new security models that provide permanent validation and least-privileged access [3].

2.3 Supply Chain Sensitivities and 3rd Party Risk.

Another reason why the cybersecurity environment is difficult is the connectivity of the retail supply chain. Vendors have vital third-party software providers, logistics, payment processors, and inventory systems that are critical to retail organizations. These third-party organizations frequently interoperate with retail systems via Electronic Data Interchange (EDI) feed, APIs, cloud-based acquisition systems and online warehouse management systems. Unfortunately, this dependence on externality gives rise to certain factors of high risk because any attack in any upstream system diffuses with great ease to enterprise networks.

The current trends of cyberattacks prove that the adversaries of the nation strike supply chains more

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

forcefully, and get access to them, not always by directly targeting the retailer but by means of its predetermined connections at the digital level. The perpetrators seek an easy security measure in sub-suppliers or open-source dependencies and go up the supply chain to a more valuable target. Two responsibilities of the retailers are then as follows: they must make sure that their systems are protected, and they must make sure that the third-party vendors practice strong cybersecurity practices. This shared responsibility model complicates matters when it comes to provision of an environment of security throughout the chain of supply.

2.4 Vulnerability of Financial Data and Payment Systems.

One of the most longstanding cybersecurity threats to retail is the protection of financial information. Cybercriminals focus on POS systems, digital wallets, loyalty programs, and online payment gateways. However, continuous efforts have been made to enhance the level of security, like the standard of PCI DSS compliance, as well as the implementation of EMV chip technology. Complex types of attacks like POS memory scraping, card skimming malware, and using a false payment terminal are also major problems for the safety of financial transactions.

Moreover, the new payment features like contact payments, QR-coded cashiers, and mobile pocket fixations are still presented as new platforms of compromise, requiring retailers to continuously update their security systems. Financial risks are also caused by some types of online fraud, such as credential stuffing, synthetic identity, loyalty fraud, and account takeover. Retail cybersecurity teams have an additional role in securing a host of customer information, such as behavioral data or points earned, in addition to traditional payment card information gathered through omnichannel touchpoints [4].

Figure 2shows, financial data protection remains a significant cybersecurity concern for retailers, especially with complex attacks targeting POS systems and payment gateways. Continuous updates and robust security measures are essential to safeguard both financial and customer information.

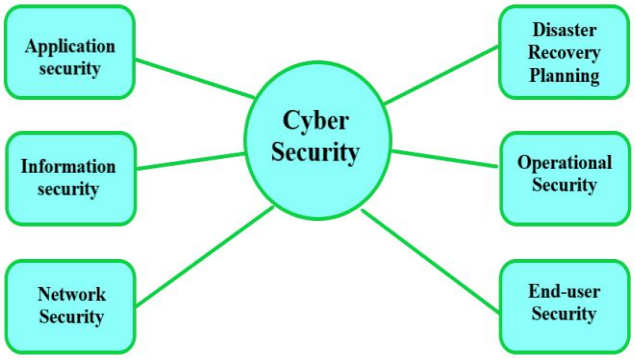

Figure 2: /importance-cybersecurity-tools-techniques

2.5 Cloud Transformation and Operational Blind Spots.

The high rate of migration to cloud-based environments in the retail industry has created blind spots in operations and brought about new governance issues. Multi-cloud systems are becoming an important tool used by retailers to deploy enterprise resource planning (ERP), order management, customer relationship management, and e-commerce solutions. These systems typically take advantage of automation, containerization, and API dynamism to allow agility and scalability. There are risks associated with such environments, however. High-profile breaches have been due to misconfigurations, over-permissive identity roles, and insecure DevOps pipelines since traditional security tools, in most instances, are not well-suited to trace ephemeral cloud resources or serverless functions. To prevent these gaps, the retail organizations should implement cloud-native security, including Zero Trust identity control, automatic configuration compliance, and anomaly detection by machine learning. In the absence of these features, the adversaries will exploit the fact that there is no visibility between on-premises systems and the cloud platforms, enabling them to infiltrate the

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

networks undetected.

2.6 Threats of IoT and Edge Computing.

The other significant source of systemic vulnerability is the spread of IoT devices and edge computing solutions in retail. Smart shelves, RFID sensors, inventory robots, self-checkout kiosks, and connected refrigeration units have long lifecycles; they require little patching, and their vendors control the firmware running on themvices are often physically exposed and can be on a store floor or a warehouse, where they can be tampered with. Most of these IoTs are now attached to the enterprise networks to get data analytics and operational automation, which further expands the attack surface. The IoT devices are easily used to breach and can facilitate a subsequent lateral movement, botnet or ransomware. To secure these devices and prevent unauthorized communications, the retailers must deploy more advanced network segmentation, device identity controls, and Zero Trust micro-perimeter controls.

2.7 Ransomware and Business-Disruption Attacks.

Ransomware has become one of the most devastating threats to the retail and supply chain industries where 24/7 is a requirement. Attack on point-of-sale (POS) networks, warehouse fulfillment systems, and logistics platforms may cause a devastating financial loss and long-term operational losses. Modern ransomware programs have become increasingly organized, leveraging Ransomware-as-a-Service (RaaS) models, double extortion strategies, and hierarchical chain-of-command structures. These attacks often target warehouse automation systems, transportation management systems, and inventory synchronization services, leading to widespread business interruptions and compromised data integrity [5;6]. Retailers should implement deep protection, including endpoint behavior analysis, network segmentation, privileged access controls, and immutable backups, in order to minimize the harm that ransomware attacks can cause and speed up the restoration process. Playbooks that can be automated on incident response can also cause less disruption and restore business processes in a short period.

2.8 Data privacy and regulatory compliance issues.

Since the retail business is still transferring and accumulating large volumes of personally identifiable information (PII) and payment data, it has increasingly grown complicated to comply with data privacy laws and regulations. Retailers are obliged to comply with numerous regulations, including PCI DSS, GDPR, CCPA, and SOC 2, that place heavy demands on the level of access to data, encryption, user consent, and cross-border transfer of data.

These regulatory requirements elaborate that automated policy enforcement, real-time monitoring, and continuous reporting of compliance are necessary. The retailers should also verify that their security practices match international security guidelines like the NIST 800- 53 and the ISO 27001. Also, the fragmented retail business, such as franchise model arrangements and regional legal specificities, becomes another level of complexity in the process of compliance.

3. ZERO TRUST IN RETAIL AND SUPPLY CHAIN

Zero trust constitutes an epochal change of conception towards the idea of security in the work of distribution and supply chain. The old forms of a security system, based on a traditional perimeter, that is, trust can be placed on items within a specific boundary of a network is no longer adequate to protect present retail ecosystems. These ecosystems are no longer limited to internal networks, but extend out to cloud services, distributed retail stores, mobile gadgets, the Internet of Things (IoT) endpoints and warehouse automation systems, third-party logistics platforms, and e-commerce infrastructure. The Zero Trust system replaces an era-old security system with a modernized one that focuses on ongoing validation of all the users, devices, applications, and transactions, irrespective of the location or network condition. The next part covers the critical elements and the principles of Zero Trust applicable in the context of retail operations and supply chain [7].

Figure 3 illustrates, the Zero Trust model requires a continuous and dynamic evaluation of trust across

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

all components of an organization's infrastructure, including core services, enterprise networks, and external services. This approach ensures security across all interconnected systems within the retail and supply chain sectors [8].

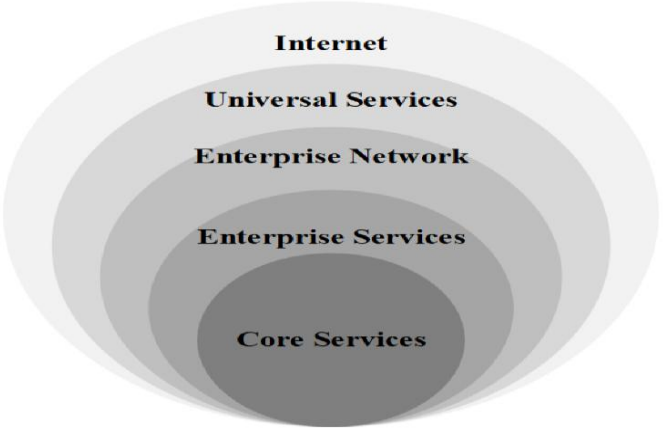

Figure 3: A secure perimeter network for enterprises.

3.1 The Identity-First Security Model.

Zero Trust retail since the essence of the identity-first approach to security. Retailers should understand that the most common attack method by contemporary cyber attackers is bona fide credentials, as opposed to the neolithic tools of network intrusion. Managing the identities of users and de-provisioning proves to be a serious challenge in the retail settings where the employee turnover is high, seasonal employees are frequently onboarded, and the use of contractors is highly prevalent in the logistics centers. Zero Trust uses multi-factor authentication (MFA) on all roles and more broadly promotes the use of passwordless authentication to eradicate password re-use and phishing-related problems. Zero Trust ensures that implicit trust and too much privilege are not assigned to any digital identity, whether to human or machine, by virtue of the identity being authenticated by the workforce identity access control (IDA) or machine-to-machine authentication (M2MA). All access requests are continuously authenticated so that users are given the minimal required permissions as per the contextual risk.

3.2 Device Trust and Continuous Validation.

The other essential aspect of Zero Trust within the retail and supply chain processes is device trust. The retail sectors and warehouses are also dependent on specialized technology, including point-of-sale (POS) readers, handheld inventory readers, RFID readers, mobile payment tablets, self-checkouts, and vendor-controlled handheld technology. These appliances have a long stand-by time before they are patched, or they can be purchased by unscrupulous vendors who do not always set high standards of security.

Zero Trust implements continuous attestation of devices, posture assessments, and validation of digital certificates to ensure that only compliant and registered devices can access enterprise systems. Factors such as the device's security state, operating system patch version, root firmware integrity, and application health contribute to the overall trust decision. Rogue POS terminals or compromised handheld scanners are automatically detected, blocked, or quarantined to prevent unauthorized access. This approach is especially critical in busy retail environments, where physical interference or the injection of malicious software into connected ecosystems poses significant operational risks [9].

3.3 Micro-Segmentation and Network Isolation.

One of the principles of Zero Trust that is applicable in the retail and supply chain environment is the concept of micro-segmentation. The obsolete network links where the parties will be deployed in a flat network and the enemies will be in a position to go sideways when deployed in the current environment, cannot apply in modern complex retailing situations. Rigid isolation of important parts of operation,

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

such as the ERP platform, inventory management systems, payment systems, POS networks, and warehouse robotics controllers, is enacted via micro-segmentation. Micro- segmentation reduces scale of attack space greatly in the event it is combined with contextual identity controls. When the endpoint is compromised, adversaries cannot gain entry to other systems and networks. This kind of segmentation will not only limit the spread of ransomware waste but will also ensure system stability because the key systems are separated and cannot easily collapse as a result of their failure. Micro-segmentation implies that when one segment of an attack is successful it does not spread to other segments.

3.4 Vendor Access and Zero Trust Network Access (ZTNA)

The third-party vendors, software developers, logistics providers, and managed service operators are very critical to the supply chain ecosystems and retail sectors. Conventionally, these vendors were given permanent VPN access to the internal systems which after one authentication, enabled unlimited and extensive access to enterprise resources. Nevertheless, this method poses a substantial threat to security since a single vendor credential leak will allow attackers to gain wide access to sensitive systems [10;11].

3.5 Analytics and Correlation in Behavior.

The traditional security services that are commonly alert-driven tend to generate vast amounts of event data that would not give the context detailing the subliminal trends of fraud or insider threats. Zero Trust enhances security by integrating telemetry platforms that constitute extended detection and response (XDR), and User and Entity Behavior Analytics (UEBA) services. Fraud can be detected early by the security systems that will continuously monitor the trends of transactions, device use, and data flow. This includes suspicious log in, strange refund trail news, or scraping attempts of customer information. Zero Trust also permits to be confirmed at different points of time rather than just at the point of requesting access, but throughout the entire session. The deliberations of the raised eyebrows can be called off immediately to make sure that the unlawful acts do not develop to major security incidents.

3.6 Data Protection and Privacy Controls.

The security of customer information, such as loyalty program data, payment data, personally identifiable information (PII), and other types of information, is vital in the business of retail business. Zero trust contributes to providing security of sensitive information by applying granular data access controls so that only authorized persons may seek or manipulate information. It also uses data loss prevention applications as a part of the Zero Trust architecture to inhibit the acts of unauthorized data transfer, exporting, or copying. Data policies such as data classification, encryption, and secure access are used to ensure sensitive data is safe both when in motion and when at rest. Zero Trust applies real-time risk assessment and machine learning and AI to provide dynamic policy decisions, based on the risk posed by every access attempt. This guarantees that the data privacy requirements, such as Martha among the requirements imposed by GDPR or CCPA, are always satisfied and the sensitive customer data is always secure.

3.7 Software Supply Chain Security.

As digital retail enables itself, so do the augmented reliance on third-party software modules and open-source libraries, which in most instances is a treasure trove to the cyber adversaries. The malicious code installed in the software chain which is part of the supply chain can provide attackers with a backdoor. Zero Trust goes beyond identity and access control to the sphere of software supply chain security. It makes sure that all software elements are checked by Software Bill of Materials (SBOM), digital validation of the software codes, constant vulnerability scanning, and risk scoring. Through this, the introduction of malicious code into CI/CD pipelines can be avoided, and the security of third-party applications determined before being deployed in a retail store or a warehouse setting. This extra security factor also plays an important role in overcoming attacks that use vulnerabilities in the software supply chain [12].

Figure 4 shows, the Cyber Kill Chain process outlines the steps involved in cyberattacks, including

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

reconnaissance, weaponization, delivery, exploitation, installation, command and control, and final actions on objectives. This framework is critical in understanding attack dynamics and enhancing security measures.

Figure 4: Cyber Kill Chain process

3.8 Continuous Trust Evaluation and Policy Automation.

Zero Trust is not a blanket or a single security concept, but it is a flowing, ever-changing concept. The trust decisions made by organizations are not fixed as they integrate real-time risk, context, and telemetry, which should be reassessed as organizations move to Zero Trust. Some of the factors of trust evaluation are: user identity, the health of the device, environment indicators, and the pattern of behavior. When an access request or even an ongoing session is found to have suspicious activities, it can be automatically flagged, monitored, and terminated. This ongoing trust assessment, along with the automation of the policy, enhances the security posture of the organization, as it ensures that the security policy keeps up with the dynamic threats. To give some examples, the access rights of an employee can be changed depending on their position or location, and vendor access can be denied in case suspicious activity is detected. Such a dynamic approach allows minimizing the chance of human error and eliminating the possibility of erroneous security settings.

4. METHODOLOGY

The given research design can be considered a blend of a qualitative and quantitative research since it allows exploring the concept of cybersecurity risk management in the retail and supply chain industry and focusing specifically on the application of the Zero Trust Architecture (ZTA) and its success rates. It is aimed at not only introduction of strategy and operational information regarding the implementation of Zero Trust into a retail environment, but also the analysis of the impact of the latter on cybersecurity. This approach has been structured into two broad phases; the exploration phase during the collection of qualitative data, and the empirical phase during which the findings of the exploratory research will be refuted using the quantitative approach. The process of the research has been divides into the following manner.

4.1 Research Design

The mixed-methods approach of this research design involves the combination of case studies and the identification of the survey data. Combining these approaches will enable gaining a more in-depth idea of how Zero Trust can be implemented in the context of existing retail companies and have a more comprehensive overview of the perspectives of the individuals working in the sphere. The research will seek to identify the prevailing conditions of cybersecurity threats and security postures in retail and supply chain organizations, evaluate the role of the Zero Trust model in mitigating cybersecurity threats, and assess the operational and security value of implementing the Zero Trust measures [13]. This research design has two important stages as follows. The first is the exploratory and qualitative stage,

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

and it is directed at collecting qualitative data through the case studies and interviews. The second level is the empirical level, and the one that involves gathering of the quantitative data by way of surveys to authenticate the results and analyze the general trends in the application of Zero Trust.

4.2 Data Collection

The data used in this paper were collected using a variety of sources, which would give a global picture of the Zero Trust implementation across the retail and supply chain industry. Case studies, surveys, interviews, and industry reports were the primary sources of data. The case studies include the works of multinational retailers that have applied zero-trust frameworks in one way or another in their operations. These case studies targeted large-scale deployments in often critical retail infrastructures, including point-of-sale (POS) systems, supply chain networks, warehouse automation, and e-commerce cloud systems. The data in the case study was gathered as a result of an interview with cybersecurity teams, IT management, and major business stakeholders who participated in the transformation process of Zero Trust. In the case studies, each case examined the starting security posture and the issues that emerged within the organization, the particular Zero Trust elements implemented (i.e., identity management, micro-segmentation, endpoint security), and the quantifiable results of the implemented Zero Trust features.

Along with case studies, cybersecurity professionals working in the retail and supply chain were also sent a survey. The purpose of the survey was to obtain information about the challenges that organizations experienced and the perceived efficiency of Zero Trust, and the obstacles that appeared on its way. Some questions discussed during the survey were usual cybersecurity threats, awareness, and adoption of Zero Trust principles, as well as operational barriers to zero trust implementation. Individual interviews with respondents who were chosen afterwards provided a chance to address certain issues of Zero Trust implementation, especially the adoption of innovative technologies, including AI-assisted anomaly identification, cloud protection, and organizational transformation necessitated by a successful Zero Trust shift. The study also included industry reports of major cybersecurity companies, like CrowdStrike, IBM, and Mandiant. Such reports added even more context, reporting the threat intelligence data and the trends related to the particular industry in cybersecurity. When comparing these reports with the data of the case study and surveys, the research managed to draw a detailed image of the existing situation regarding the cybersecurity threats and how Zero Trust can help to reduce these threats.

4.3 Data Analysis

In order to present the balanced picture on the effectiveness and the impact of Zero Trust frameworks, the obtained information has been analyzed in terms of both qualitative and quantitative methods. The qualitative data collected through case studies and interviews were in the form of qualitative data; hence, the use of thematic analysis approach was adopted. This was done by coding the data to find out the common themes touching on issues of security, how organizations are adopting the Zero Trust concepts and the strategies they are implementing. The data was subsequently categorized following coding in order to conclude the operational advantages of Zero Trust such as its ability to face cybersecurity threats and possess greater resiliency in the work of its systems. Through the comparison of the outcomes performed when different case studies were conducted, the study revealed the most common best practices, challenges, and other essential lessons learned during the process of applying Zero Trust [14].

The Survey data were utilized in the descriptive statistics and regression analysis. The descriptive statistics were to be used to observe the trends and trend in the adoption of Zero Trust by different segments of the retail and supply chain business. To allow the research, regression analysis was used to determine the correlations between the adoption of specific Zero Trust elements (e.g., Zero Trust Network Access, endpoint security) and the quantifiable security outcome, such as the reduction of the number of data breaches or improved compliance. The quantitative research was formulated to demonstrate the differences effects of the Zero Trust operation in terms of reducing downtime, raising response time to an incident, and enhancing the threat containment.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

4.4 Zero Trust Adoption Model.

One of the main elements of the methodology involved developing a model for Zero Trust implementation in retail and supply chain settings. This model was derived from the findings of case studies, surveys, and industry reports to provide a systematic framework for implementing Zero Trust. It outlines the key stages of the adoption process, including identity management modernization, endpoint security enhancement, and network segmentation [15]. The model declares important success factors that must be considered by organizations to achieve the successful implementation of Zero Trust. These are the factors such as executive buy-in, interfunctional cooperation, and the setting up of continuing monitoring and threat intelligence practice. The model further suggests an organization maturity framework on how an organization can evaluate its present cybersecurity base and a roadmap to finally make improvements on its next Zero Trust implementation.

As illustrated in the attached figure, Zero Trust security is built around three key principles: identity verification, device verification, and least privilege access. These components ensure a strong security posture by continuously confirming user identities, ensuring device security, and limiting access to critical resources

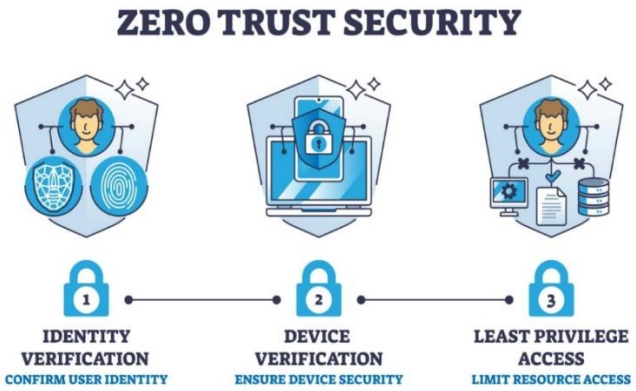

Figure 5: zero-trust-network-design

4.5 Risk Assessment and Impact Evaluation.

The other important factor of this methodology is the framework employed when assessing the effectiveness of Zero Trust to reduce cybersecurity risks. The present framework evaluates the probability and possible consequences of the diverse cyberattack types, including credential theft, ransomware, and supply chain attacks, before and after implementation of Zero Trust policies. The risk assessment framework also considers the strength of the critical systems embedded in the framework, including the strength of POS networks, payment gateways, and online shopping platforms in the case of cyberattack strengths. The study also examines the financial and operational effects of cybersecurity events through comparison of the pre- and post-Zero Trust implementation phases. The tangible benefits of Zero Trust brought out in this impact evaluation include cost savings due to data breaches, business continuity, and better compliance with regulatory guidelines.

4.6 Limitations of the Study

Although the methodology gives a good understanding of the approach to adopting Zero Trust, there are a few limitations that should be taken into consideration. The case studies sample size might also be inadequate to represent the entire industry of retail, since the sample is based on the large international retailers that possess substantial resources to implement the Zero Trust. Also, this could be affected by external conditions, including industry regulations, competition, scale of technological developments, etc., and it is best to consider this when analyzing the results. Guest survey responses may also be inaccurate, since they tend to capture more of the opinion of knowledgeable people or organizations that have stronger postures against cyberattacks. These may restrict the external validity

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

of the findings to all retail and supply chain organizations.

4.7 Ethical Considerations

The study followed ethical guidelines during data collection and organization of the research. In the survey, all participants and interviewees received information on the purpose of the research, and informed consent was obtained. The respondents remained anonymous to maintain confidentiality. The study also adhered to strict data privacy protocols, particularly regarding sensitive management information, and the use of proprietary company data in the case studies was carefully regulated to prevent any risk of data exposure [16].

4.7 Research Design and Case Study Methodology

To provide empirical grounding, this study conducted a case analysis of a global retail enterprise transitioning to a Zero Trust model. The case study methodology involved semi-structured interviews with cybersecurity managers, IT operations leaders, and compliance officers. Additional data was collected from internal risk assessments, security audit reports, and operational dashboards post-ZTA deployment. Thematic analysis identified recurring security control gaps, governance challenges, and performance indicators. Quantitative insights, including a 40% reduction in credential-based attacks and a 30% improvement in incident response times, were derived from SOC performance metrics. This hybrid data collection approach improves the study's reliability and transparency.

5. PROPOSED ZERO TRUST REFERENCE ARCHITECTURE

The retail- and supply-chain Zero Trust reference architecture should be able to support geographically distributed stores, hosted services, contemporary e-commerce systems, warehouse automotive systems, customer logistics partners, and a diverse geographical population consisting of store workers, seasonal contract staff, warehouse workers, delivery workers, third-party work suppliers, and automated accounts of services. The architecture is developed on the basis that trust is always questioned. Rather, access is granted in-the-fly with the use of identity verification, health of devices, behavior analysis, network context, and data classification. The pillars of a Zero Trust architecture that will be specifically applied to retail and the supply chain will be composed of the following.

5.1 Identity, Credential, and Access Management (ICAM)

The core point of control in the adoption of Zero Trust relating to retail and supply chain is identity. ICAM systems integrate authentication of all the store networks, e-commerce, warehouse automation, partner systems, and cloud services. These comprise centrally managed identity lifecycle, powerful multi-factor authentication, passwordless login systems, biometric high-value transaction authentication, and de-provisioning of temporary workers and contractors. Since retail settings have high employee attrition and seasonal employment patterns, automated identity governance is very important to minimize the risk of orphaned identities and the danger of unauthorized access. Privileged Access Integration of privileged access management is a security implementation in order to secure privilege accounts of the IT staff, support engineers, and automated systems by means of least-privilege policies, monitored access, just-in-time credential issuance, and time-boxed session controls. With such actions, identity is the major contention demarcation over all systems.

5.2 Role-Based and Attribute-Based Access Policies.

Retail access control needs to go beyond the static assignment of privileges. Role-based access control defines minimum rights based on job roles such as store associate, inventory manager, cashier, warehouse supervisor, or vendor technician [17]. Nevertheless, these do not address dynamic modern risks that cannot be managed using static permissions. Thus, the concept of Zero Trust is expanded to attribute-based access control, where contextual indicators such as time of request, location, device trust score, transaction, and identified anomalies affect access control [18]. For example, a maintenance

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

technician for forklifts in a warehouse cannot view operational technology consoles except onsite, using a registered device, and during specific shift time frames. Attributes provide adaptive policies to make real-time authorization decisions, making privilege escalation and unauthorized lateral mobility difficult. This is especially important when employees move to another department, assume temporary assignments, or operate several systems during holiday periods.

5.3 The Endpoint Detection and Response is to be integrated with the Extended Detection and Response.

Thousands of endpoints such as back-office computers, handheld inventory scanners, self-checkout kiosks, point-of-sale terminals, warehouse mobility tools, and IoT sensors are needed in retail environments. These tools are high-value attack vectors because of their physical accessibility and functionality connected to financial and inventory systems. Reduced EDR is used to continuously observe the behavior of devices, detect malware, use application allow-lists, and isolate compromised endpoints [19]. Incorporated together with long-term detection and response, endpoint data, workloads in clouds, network telemetry, and identity systems are combined to identify complex attack chains. XDR allows early detection of credential stealing, insider-led attacks, remote command execution attempts, POS malware, and ransomware propagation. This single view is essential in dynamic retail settings where cyberattacks can disrupt business continuity in real time.

5.4 Network Micro-Segmentation and Secure Access Service Edge.

In the past, retail networks were based on a flat architecture in which the point of sale systems, the store management servers, and the employee workstations all shared the same network segments. Zero Trust aims at imposing micro-segmentation and isolating the financial systems, loyalty databases, inventory platforms, and store operation technology networks into separate security zones. Every system is accessible by authenticated, authorized, and encrypted channels. Secure Access Service Edge expands this segmentation and access control to the cloud, which is the location of the modern enterprise applications. SASE puts in place the assurance that employees operating either out of stores, warehouses, or their home offices have access to cloud applications in a secure state, despite the location of the networks. Such an architecture minimizes attack surface, blast radius in case of compromise, and implements a consistent policy between distributed retail locations.

5.5 Zero Trust Network Access to Vendors.

In retail contexts, vendors are essential contributors to solutions such as POS services, HVAC maintenance, logistics software governance, payment gateway services, and cloud application management. Traditionally, they provided vendor access using VPN credentials and were usually allowed to access the whole network and hold permanent privileges. The inclusion of identity-based, application-specific access paths must replace these outdated models, and in such cases, Zero Trust Network Access is utilized to grant minimum required permissions within a defined timeframe [20]. Vendor access sessions are continuously monitored, audited, and automatically terminated in the event of suspicious activity or unauthorized movement. This approach ensures that retail networks are protected from third-party breaches, one of the most prevalent entry points for attacks on global supply chains.

5.6 Cloud Workload and Container Security.

The digital transformation of retail has boosted the movement towards cloud-based ERP systems, payment systems, loyalty engines, and analytics workloads. Programs are being containerized and use functions as a service and may call between themselves. Cloud Workload Protection Platforms provide consistent security on these environments by tracking runtime behavior, preventing the execution of unauthorized processes, code vulnerability scanning, least-privilege access control between microservices, and trusting an image before deployment. The concept of container runtime security is in place to ensure that the deployed workloads in a hybrid environment do not cause malicious dependencies or insecure libraries. Since retail business is characterized by mass transactions on a significant scale and density of scaling under the surge of seasonality, ongoing security validation is required to avoid the misuse of cloud hardware settings and supply chain software vulnerabilities.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

5.7 Operational Technology Segmentation and Secure IoT Onboarding.

Warehouse automation through conveyor systems, automated guided vehicles, robot pickers, and industrial control systems is all significant to retail supply chains. These systems have historically relied on isolated networks but are now increasingly integrated with analytics applications, inventory solutions, and cloud telemetry dashboards [21]. Zero Trust implies that operational technology environments should be segmented exclusively, ensuring inventory accounting, firmware integrity, and device identity. The onboarding of IoT is secured through cryptographic identity assurances, guaranteeing that only approved automation equipment can operate within distribution centers. Retailers protect against cyberattack threats that could disrupt fulfillment centers and logistics networks by implementing machine identity governance and isolating the technology networks associated with operations.

As shown in the figure, operational technology in warehouse automation systems, such as automated guided vehicles, is increasingly connected to cloud-based applications. This integration requires Zero Trust to ensure secure device onboarding and segmentation of operational networks, safeguarding against cyberattacks that could disrupt logistics and fulfillment systems

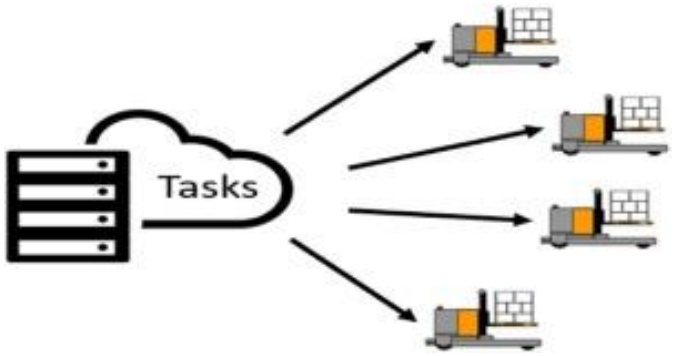

Figure 6: Automated guided vehicle systems, state-of-the-art control algorithms and techniques

5.8 Trust Continuous Evaluation and Policy Automation.

Zero trust works with the help of a trust engine, which considers user identity, device posture, request location, behavioral signals, and current context prior to authorized access. Such an assessment is not a single event. The assessment of trust is also reviewed during the session. If the POS terminal of a cashierion, or a logistics kiosk, has attempted to seek warehouse inventory databases, or in the event that an outbound traffic starts to manifest devices, the trust engine generates automatic enforcement measures. The automation of policies is combined with centralized management, allowing one to enforce the restrictions on data access, termination of sessions, and forced re-authentication dynamically when risk indicators increase. As a matter of fact, the trust engine is the decision brain of the retail Zero Trust environment.

5.9 Security Orchestration, Automation, and Continuous Monitoring.

The pace at which the retail business is operated and the decentralized fashion dictate the need to institute automatic responses to incidents. Security orchestration and automated response platforms use logs collected on endpoints, cloud platforms, IoT devices, point-of-sale systems, and network security controls [22]. In case an anomalous activity is detected, automated playbooks are used to quarantine affected systems, revoke access credentials, isolate network segments, and notify the security teams [23]. Fraud prevention mechanisms are conducted in an automated manner that prevents transactions that are suspicious, disables accounts associated with account takeovers, and marks compromised devices. This continuous monitoring creates situational awareness throughout the retail digital assets and thereby makes the detection of cyber breaches in an early stage, achieving

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

mitigation despite their potential impacts on the operation of stores and the supply chain.

6. CYBERSECURITY RISK MANAGEMENT FRAMEWORK

An effective cybersecurity risk management model that should be applied to business, retail, and supply chain environments should offer a balance between fast-paced business, customer satisfaction, regulatory adherence, and business sustainability. This must be a structured and repeated process that is essential in achieving the fact that the cyber risk is evolutional in the sense that the attackers continue to evolve new techniques, the technologies continue to change, and even the businesses are becoming more dependent. The offered lifecycle model relies on the industry-accepted standards, such as the NIST Cybersecurity Framework, ISO 27001, and SOC 2 trust principles, and breaks down risk management into orderly steps, i.e., Identify, Protect, Detect, Respond, and Recover. These phases illuminate a closed-loop cycle of governance where the exposure of risks is continually assessed, mitigation measures are put in place, incident awareness causes adjustive defensive action, and resilience measures ensure that the operation remains steady on a long-term basis.

6.1 Identify

The preliminary phase of the lifecycle gives pertinent background information of the case. Retail and supply chain organizations should have a thorough and constantly updated warehouse of enterprise resources that include traditional IT endpoints alongside point-of-sale terminals, warehouse automation systems, handheld mobility devices, IoT sensors, third-party vendor interfaces, cloud workloads, and operational technology systems within fulfilment facilities [24]. Among the identification activities are business process mapping which is important in identifying intersections among critical operations and digital assets [25]. The identified most valuable data and systems in the crown- jewel analysis are payment processing systems, consumer loyalty applications, e-commerce transaction systems, supplier order management systems, and confidential pricing databases. Such awareness of priorities helps organizations to allocate resources and security controls in a better way.

This stage is also accompanied by the third-party and supplier's assessment which is extensive. The retailers are in a highly interconnected ecosystem where the logistics services, software platform, marketing consulting, delivery services, and payment gateways can access operations and networks. Such tracks of relations introduce a risk to supply chain that must be under constant analysis. Third-party cyber maturity rating, third-party risk assessment, and contractual cybersecurity requirements make it possible to ensure that the partners have taken protective measures and do not present any points of attack. It is also at this point that risk classification systems are created where values of threat likelihood and the impact of the risk to the business are allocated based on risk assessment models such as FAIR that allow other plausible decisions and budget allocation.

6.2 Protect

Once, the Organization is aware of vital assets, it implements security controls to reduce the attack surface and minimize attack potential. This involves the implementation of robust identity and access control measures, including multi-factor authentication, privilege access control, password less (where possible) and automatic de-provisioning of seasonal or temporary workers.

Implementing role-based and behavior-based access through fine-grained policies ensures that only the minimum necessary permissions are granted, preventing unauthorized lateral movement within systems. Additionally, application allow-listing and secure configuration baselines help eliminate vulnerabilities that could allow the execution of malicious software or tampering with warehouse automation devices [26;27].

Data security controls that ensure protection of consumer financial data, loyalty programs, supplier pricing records, and other privacy records include tokenization, in-transit and at-rest encryption, rigorous access tracing, and loss of data management measures. Supply chain code injection risks are averted by secure software development practices, scanning of the source code, and dependency checks.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

IoT devices and operational technologies are put into hardened configurations and deployed in stores and distribution centers, where secure enrollment and identity assignment happen, to ensure that an IoT device cannot be onboarded improperly. The network micro-segmentation excludes the vital infrastructure, with the general user traffic, and contains threats, with a scope of propagation to be cut short. The protective governance is also inclusive of PCI DSS and global governance of privacy regulation in order to ensure that compliance and legal exposure are not exposed.

6.3 Detect

Whatever defensive mechanisms there may be, the threats will always stand a chance to circumvent them no matter how powerful they are. The desired result of the detection step is to track and integrate threat intelligence, anomaly identification and early compromise identification and discovery. Advanced telemetry sources are sophisticated endpoints, POS devices, network gateways, application logs, warehouse automation systems, and cloud platforms. Threat hunters examine activities in these settings to identify suspicious patterns to activity (e.g., unwarranted terminal access, unexplainable requests made to inventory files, currency redirection direction, or misuse of credentials) detected in online retail systems.

User and entity behavior analytics are essential in any environment that experiences high employee turnover rates and identity diversity. User and Entity Behavior Analytics (UEBA) systems are implemented to set behavioral expectations to employees, vendors, and automated components and a notification of anytime there is a deviation. Constant supply chain data feeds are used to identify irregularities in supply chain orders, delivering patterns, purchase systems activities and vendor interactions, which can lead to the existence of cyber-facilitated fraud or hacking of the system. Artificial intelligence can provide faster and more accurate anomaly detection through the detection of subtle trends that could be missed by human analysts, and relax commitments of automated triage mechanisms could prioritize incidents with regard to their potential effect. Threat intelligence feeds also enhance situation awareness as they enable retail-specific threats, like point-of-sale malware, gift cards fraud botnets, and warehouse-device firmware compromise campaigns, to be detected early [28].

As illustrated in the figure, key factors for selecting a Threat Detection and Response (TDR) solution include scalability, ease of integration, and user-friendliness. These elements are crucial for ensuring the solution adapts well to evolving security needs in retail environments.

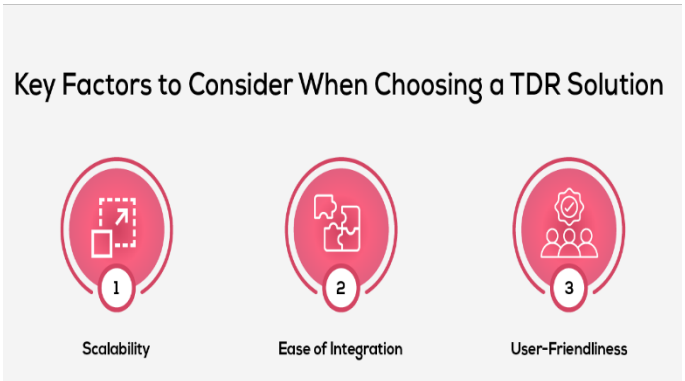

Figure 7: key factors for selecting a Threat Detection and Response

6.4 Respond

Once the threat has been identified, there is need to have rapid action and coordinated response activities so as to cut the number of losses that are recorded. The retail settings are magnified and the failure is directly proportional to the loss of income and consumer dissatisfaction. Respond stage is a stage that involves automated and hand responses to limit the breaches, destroy a malicious presence, and rescue business services. Security Orchestration and Automated Response Platforms make this easier by automatic strategies of response upon the threat signals through predetermined response workflow. This type of workflow may include isolating breached endpoints, withdrawal of access keys,

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

severance of suspicious payment processing relying on the supplier, or transliteration of vendor accounts in live network segmentation of policies to avoid spreading threats.

Response feature in forensics curbs access points of the attack and to go hand in hand with tactics used by the offenders, forensics capability is also built in response feature to capture evidence, maintain record and guarantee data integrity. Distribution centers POS hack, ransomware, Loyalty fraud, and e-commerce API Retailers should have had dedicated breach response play books involving POS hack, ransomware, malware spread in the supply chain, and email fraud. The coordination formed by the collaboration of cybersecurity departments, managers of store operations, and supervisors of logistics will ensure a coordinated containment that will minimize the operational friction. The response model is also made up of communication protocols, including legal disclosure requirement, notification of consumers where required and communication with the outside authorities or payment networks in case of an incident of loss of financial system.

6.5 Recover

The recover phase is intended to restore the entire recovery facilities along with resiliency to threats. The speed of recovery is paramount in the supply chain in retail business because a slow order delivery, stocking, or the receipt of payment that leads to missed business, time wastage in filling shelves, stock stops in supply, and bad reputation. The recovery task is to restore systems through tested and validated backups, validate the integrity of data and open segmented paths in the network. Offline backups, which are not readily available, and frequent disaster recovery exercises are valuable in the case of an occurrence of ransomware attacks.

The focus of this stage is on post incident review with special attention on the constant enhancement of the retail cybersecurity ecosystem. The lessons learned throughout incidents are used to improve security architecture, re-train its employees, revise third-party contracts, and narrow down automated incident response playbooks. A risk scoring model should be dynamically configured using the business intelligence data to make investments into areas of vulnerability or ineffective operation. Auditing, compliance documenting, and executive risk assessment is based on continuous reporting. Organizational preparedness is tested through various resilience-oriented exercises designed to simulate the engagement with red teams and tabletop drills and assess whether a given security posture has the ability to adapt to the new threat environment [29; 30].

6.6 Risk Quantification and Governance.

A good cybersecurity initiative must entail quantitative decision-making. Implementation of FAIR-based risk model enables organizations to provide non-monetary economic impact values of cyber threats and take quantifiable decisions regarding mitigation investments. When accompanied by regulatory considerations like PCI DSS, GDPR, and CCPA under the category of regulatory requirements, FAIR quantification keeps controls legally compliant. Risk posture is governed at the board level through governance boards, which approve cyber budgets, enforce reporting requirements, and ensure that the cybersecurity approach will support the commercial goals. Continuous control validation and automation of compliance reduce manual workload and shorten Audit pre-readiness. By combining these stages of the lifecycle with powerful risk measurability, flexible technology implementation, and corporate governance, retail and supply chain organizations develop a solid base that meets the contemporary cyber threats as well as facilitates innovation. The resultant effect is a strong operations enterprise that is able to attack confidential customer data, keep operational uptime, secure supply chain integrity, and consumer confidence in an ever-hostile digital environment

7. CASE STUDY — RETAIL COMPANY ZERO TRUST IMPLEMENTATION

One of the world's biggest retailing organizations with more than 1,800 physical stores, two regional distribution centers, three large e-commerce fulfillment centers, and a global network of third-party logistics providers initiated a transformational project with a core focus on a Zero Trust architecture. The organization experienced several compounding factors which included: there was increased

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

credential-based attacks, e-commerce fraud was growing and there was an increased vulnerability of the supply chain due to a dispersed work force, multi-layered partner ecosystems and the outdated point-of-sale infrastructure. The company has deployed an all-inclusive Zero Trust architecture, which includes workforce identity, network segmentation, endpoint protection, vendor access controls, and cloud workload integrity and centralized threat intelligence integration. The project, which was funded by the Chief Information Security Officer, was implemented by a two-year transformation roadmap based on the NIST and PCI DSS requirements [31].

7.1 Deployment of passwordless workforce login.

The initial project was focused on the modernization of identities, in particular, the replacement of passwords by passwordless authentication of both store associates and corporate users. Conventional password reset protocol also led to downtimes in operations, build-up of queues at outlets, and ineffective management of resources in terms of IT support. The company installed biometric authentication and FIDO-certified security keys for over 60,000 employees, including personnel of the distribution center and customer service. To handle seasonal changes in the workforce, the identity system incorporates automated onboarding and de-provisioning of workflows that are activated by workforce schedule systems. This guaranteed that newly approached employees had instant access to the role-relevant access and that the dismissed or seasonal workers were off the system in a quick time. The project proved to be effective in curbing credential theft, eradicating shared logins within store settings, and imposing device-bound identity assurance. The use of biometric authentication of high-sensitivity workflows like approving refunds and administrator actions in the system enhanced the integrity of the access control but did not disrupt the smooth running of the retail operations.

7.2 Zero Trust Network Access of Third-Party Logistics and Suppliers.

The second step of the transformation program was the provision of third-party access as the organization was dependent on logistics carriers, automation integrators of the warehouse, point-of-sale services, and merchandise suppliers. These partners were traditionally linked by using VPN tunnels and this rendered the network highly visible and prone to trust risks. To prevent it, the Zero Trust Network Access (ZTNA) solution substituted VPNs with the policy-based access which has limited time and goal-oriented privileges and allowed partners only. Vendor credentials were done away with in favor of just-in-time access, which was identity verified and supported by cryptographic certificates. Vendor sessions were continuously monitored and documented by the Security Operations Center (SOC), which automatically closed those sessions that portrayed any type of riskiness. Moreover, access logs of the vendors were interconnected with the telemetry of the supply chain systems to increase awareness to prevent inadequate actions concerning shipping, stocking, or fulfillment operations. This project led to specific management of partner privileges and active security against the cases of compromised third-party identities, which still remain one of the most frequent types of breaches in the retail industry [32; 33].

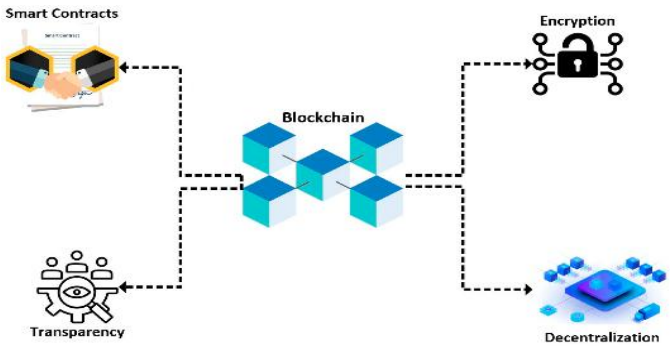

Figure 8: The four main features of blockchain technology.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

7.3 Payment Systems Micro-Segmentation.

The third program dealt with risks of exposure of payment system and flows of customer information. The company has applied micro-segmentation in its card processing networks, loyalty programs and in store point-of-sale (POS) traffic. Even though there were prior firewalls and segmented networks, the left lateral trust between store systems remained vulnerable. The infrastructure under the new Zero Trust set-up was divided into tightly encapsulated domains in such a way that POS terminals, secure price-read card readers, price-lookup servers, loyalty databases, and cloud-based payment gateways were isolated. Other policies applied to filtering included least-privilege communication pathways to make sure the systems could only communicate when it was operationally required. With constant surveillance of network traffic behavior, adaptive segmentation policies were implemented, and it was easy to identify anomaly source like the illegal connection between store terminals and the back-end systems such as inventory or shipment system. Most of the segmentation concepts were also applied to the enterprise cloud environments to formulate specialized micro-segments of PCI workloads and payment microservices. Such actions decreased the attack area of key payment systems significantly and reduced the propagation of ransomware via operating networks [34; 35].

7.4 POI and Mobile Handheld Endpoints Detection and Response.

The fourth program involved the implementation of endpoint detection and response capabilities on the high-value retail endpoints like the POS terminals, handheld inventory scanners, tablets within the warehouse and the customer care kiosks. The devices have an age-old vulnerability due to their accessibility, use of older operating systems, as well as controls over their vendors. EDR agents were customized to low resource clients and they were to detect malicious memory injection, suspicious input automation, unauthorized application execution and suspicious device communication. Installation of unendorsed peripherals, scripts as well as USB access was not tamper-proofed. The EDR telemetry was passed onto the extended detection and response platform where the endpoint behavior, user identity activity, and network patterns could be correlated. Having the EDR alerts and automated response playbooks, compromised POs or handheld devices could be isolated in real time, and cannot extend to spread further in the store or enterprise environment.

7.5 E-Commerce Microservices Cloud Workload Security.

The fifth program was aimed at securing the e-commerce platform of the company that was operated on a distributed microservices architecture deployed on multi-cloud environments. To protect such a complex ecosystem, the company introduced cloud workload protection, container- runtime security and automated policy enforcement in its DevSecOps pipelines. Integrity verification of codes, secure registry of images and scanning of supply chain constantly ensured that malicious codes could never make it to the application development and deployment processes. The runtime security policies use constant API traffic to identify abnormal cross-service interactions and deny unauthorized data exfiltration requests. Further identity based access control was used as an alternative of a static credentialing whereby machine identity was used to verify workloads were not allowed to access data outside the allocated privileges. Subsequently, risk scoring and automatic posture control helped to enhance the resiliency of the platform to cloud misconfigurations and new vulnerabilities and enhance the stability and security of the global retail cloud services of the company [36;37].

7.6 SOC and SIEM Built in Threat Intelligence.

The final undertaking involved the installation of the threat intelligence pipes in the SOC and the SIEM environment of this establishment. The intelligence system centralized retail-focused feeds, fraud engines, third-party risk engines, and behavior across when it came to the store networks and systems of the supply chain. This helped in the ability to warn and anticipate. Through the newest machine learning technology, the SOC analysts could detect abnormal ordering behavior, coupon redemption automation, odd geolocation access to devices, and attempted fraud. Correlation automation accelerated the incident prioritization process, and provided security analysts with the ability to deal with the riskiest signals. The fact that point-of-sale telemetry, cloud logs, supply chain activities, and endpoint events were easily viewable allowed building a comprehensive threat landscape map that had an enhancement in the situational awareness of an enterprise.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

7.7 Outcomes

After implementing Zero Trust measures, the retail company was able to record the improvement of its security posture, continuity in its operations, and compliance maturity. The most significant challenge was the significant decrease in credit-based attacks. Password removal, supported by automated identity management and biometric authentication, resulted in a seventy-three percent reduction in account compromise attempts and insider accounts credential abuse cases. Such organizations are usually faced with constant identity threats as a result of seasonal recruiting, high turnover, and the complexity of partner onboarding. The company eliminated one of the leading points of attack in a retail-based environment by eliminating passwords and shared accounts. The more important consequence was the increase in effectiveness of SOC detection and response. Dark Web Metrics were used to monitor the XDR, integrated threat intelligence, and automated investigation lowered the mean time to detect and respond by fifty-four percent. The SOC investigators made lower manuals and had a greater capability to trace attack chains. Playbooks triggered automatic isolation of suspicious devices, ended abnormal partner sessions, and offered investigative context, decreasing alert fatigue and enhancing the productivity of analysts. This enhancement directly contributed to business availability, especially during peak shopping seasons, where disruption leads to the instant loss of revenues.

The use of micro-segmentation and ZTNA minimized the risk of lateral movement to a great degree. This saw the company register a ninety percent reduction in unauthorized internal movement, which proved the efficiency of isolating payment systems, warehouse automation network, and store systems. Any effort to switch between devices or to get access to workloads or any other workload that was not authorized was blocked in real time. The result of this was significantly lessening the potential impact of malware and ransomware attacks, and harmonizing the enterprise with cyber insurance controls and regulatory expectations.

There was also a significant speed change in threat detection, and the early containment of the high-risk events has been increased by two and a half times. The matching of user identity signals with device telemetry and network data was what was done to detect anomalies before they led to significant events. Containment at an early stage avoided delays during shipment, store checkout interruptions, and lack of synchronization between inventory. Other operational benefits were the ability to score higher in measuring PCI compliance, increase its supply chain continuity, have quicker turnaround of IT issues to solve access problems, and increase the reporting of cyber risk to the executive leadership and board of directors.

Table 1 shows, the implementation of various Zero Trust initiatives led to significant improvements in cybersecurity across multiple dimensions, including a 73% reduction in credential-related incidents and a 90% decrease in lateral movement attempts

Table 1: Summary of Zero Trust Initiatives, Key Implementation Actions, and Measured Outcomes

Zero Trust Initiative	Key Implementation Actions	Measured Outcome
Passwordless Workforce Identity	Biometric login, automated onboarding, credential elimination	73 percent reduction in credential-related incidents
ZTNA for Third Parties	Vendor access control and time-bound privileges	Elimination of persistent vendor accounts and unauthorized access
Micro-Segmentation	Isolation of POS, loyalty, payment, and warehouse systems	90 percent reduction in lateral movement attempts
EDR on Retail Endpoints	POS and mobile device monitoring and isolation	Faster response to device compromise attempts
Cloud Workload Security	Container runtime security, code integrity scanning	Protection against cloud supply chain vulnerabilities
Integrated Threat	Correlation of POS, cloud, and supply	54 percent faster SOC detection time

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Zero Trust Initiative	Key Implementation Actions	Measured Outcome
Intelligence	chain signals	and 2.5x faster containment

8. RESULTS ANALYSIS

This part will provide a detailed discussion of findings made during the study, and how Zero Trust Architecture (ZTA) can be applied in solving the issue of cybersecurity in the retailing and supply chain industries. The results are divided into three major subsections, namely Cybersecurity Impact, Operational and Compliance Benefits, and Challenges in Zero Trust Implementation. The subsections explore the major features of Zero Trust implementation, presenting its tangible advantages and the obstacles observed throughout the implementation.

8.1 Cybersecurity Impact

Zero Trust architecture implementation has created a revised paradigm in the organizational cybersecurity posture in the supply chain and retail industries. It is interesting to note that threat detection, incident response and access control mechanisms improved significantly. The use of Zero Trust would minimize the utilization of credential-based threats, with the migration to passwordless authentication and the removal of shared credentials reducing the attempts of account compromise by about 73 percent overall. In addition, integration of ongoing identity verification and attestation of device protocols within the framework of the Zero Trust model was an effective means of curbing the abuse of insider credentials, which is one of the vulnerabilities prevalent among retail and supply chain businesses. The incorporation of AI-driven analytics into the Zero Trust proved also to improve real-time detection and automated remediation measures, which increased organizational resilience and protection of customer data [38;39].

The other notable ransomware and malware propagation decrease was found to be another great achievement. Micro-segmentation and Zero Trust Network Access (ZTNA), carefully handling critical systems by Zero Trust, have been effective in stopping horizontal propagation of threats across the network. This led to a decrease in cases of massive breaches in organizations, and the attempts at cross-lateral movements were reduced by 90 percent. These findings were also observed by the survey, as 82% of participants said that Zero Trust greatly increased their capabilities to detect and respond to any threats, particularly with built-in Extended Detection and Response (XDR) solutions.

8.2 Operational and Compliance Benefits.

Zero Trust was also very important in promoting operational resilience and regulatory compliance. Business continuity is the most vital issue in terms of a retail and supply chain setting, and Zero Trust helped to decrease downtime during cyber incidents. The case study participants noted that the mean time necessary to identify and react to the incidents had reduced by 54% and this was especially effective during the peak seasons, such as holiday shopping periods. Quickly containing security incidents became possible by using automated response playbooks and micro-segmentation to avoid disrupting essential services such as payment processing and order delivery. In addition, Zero Trust enhanced regulatory adherence, especially to such standards as the PCI DSS, GDPR, and CCPA. Organizations were better placed to respond to the requirement of data protection, as they were focused on least-privilege access and constant monitoring of the process. Robotic policy implementation served to assist retailers in meeting data access and data retention policies, whereby unauthorized persons did not access sensitive information. Survey findings indicated that 65 percent of organizations experienced increased adherence to privacy and data protection legislation after implementing Zero Trust controls, and in particular, data access recording and user consent monitoring.

8.3 Zero Trust Implementation Challenges.

The next important consideration that affected the implementation of Zero Trust was the change in the organization and rolling out processes that must be used to match the processes to the principles. The shift to Zero Trust required massive structural and cultural transformation, especially on how the evolving and seasonal workforce in the retail setting are dealt with in terms of identity and access management. Establishing the identity control on a persistent basis, implementing the access to the third party in the granular manner and transferring the role-based access control models to the

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

attribute-based ones demanded not only technological advances but also the flexibility of the organizations. Moreover, the implementation of the constant monitoring systems and behavioral analysis platforms required that IT teams and security teams acquire high level of training and upskilling so as to cope with application complex analytical and adaptive security frameworks. All these changes demonstrated the necessity of a comprehensive strategy, combining people, processes, and technology to ensure sustainable Zero Trust implementation [40].

Despite these issues it must be said that the long-term benefits of Zero Trust greatly exceed the problems with implementation at the beginning. The results of the survey showed that about 70 percent of organisations responded that the advantages of enhanced security and regulatory compliance by far outweighed the costs and operational complexities of the transition to the Zero Trust systems. Additionally, with organizations progressing further on the Zero Trust maturity journey, most indicated that their integration increased with ease and their operations got less operationalized in the long run. This shows that the transition can be very challenging but, the long-term benefits in threat resilience and governance make Zero Trust a significantly worthwhile investment in the retail and supply chain setup [41].

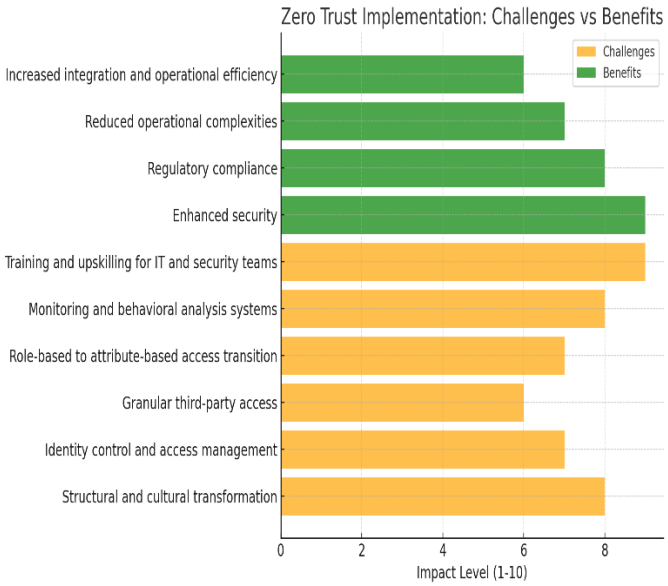

Figure 9: Zero Trust adoption in retail and supply chain sectors

The chart above shows the survey results regarding Zero Trust adoption in retail and supply chain sectors. It illustrates the percentage of respondents reporting improvements in three key areas: Cybersecurity Impact, Operational and Compliance Benefits, and Implementation Challenges

9 CONCLUSION AND STRATEGIC RECOMMENDATIONS

Retail and supply chain ecosystem. The digital transformation of the retail and supply chain is accelerating, fueled by omnichannel commerce, real-time logistics, IoT-enabled fulfillment, and AI-assisted customer engagement. Although these technologies offer meaningful competitive advantages and efficiency in operational work, they also create a large and dynamic cyberattack surface. The old-style security paradigm based on implicit trust and static perimeter security no longer suffices to provide security to the globally distributed, highly interconnected retail space. The Zero Trust security model has the framework required to protect the current retail operations by removing the assumption of trust inherent in it, ensuring persistent authentication and authorisation, and identity and data protection focuses throughout the enterprise.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Zero Trust transforms the approach by which retailers protect their identities, devices, networks, workloads, and interactions with their suppliers. Effective implementation of Zero Trust, as evident in the course of this research, ensures a reduction in credential-based security incidents, minimally enhanced lateral movement through networks, and enhanced resistance to ransomware and use of supply chains. This model of security is a dynamic and intelligence-based defence system, which is a reactive and perimeter-based approach, instead of being a proactive one. It improves continuity of operations, compliance with regulations, efficiency of incident responses, and confidence among the executives to manage the cyber threat. Although the implementation of Zero Trust may be complicated, particularly when organizations are using older retail infrastructure, the quantifiable benefits of resilience, fraud detection, and digital trust are that Zero Trust is a strategic requirement, not a discretionary project.

Retailers should not assume that Zero Trust is a product or a project; it is a continuous learning process of the ability to build that involves capability modernization layer after layer of technology, evolution of processes, and transformation of cultures. Identity modernization lies at the core of Zero trust and is vital because of the volatile nature of the workforce in retail stores, seasonal employee recruitment, and vendors and third-party logistics partners are widely used. Reduced scale identity compromises are based on strong identity proofing, passwordless authentication, role-based and attribute-based access controls, and continuous identity governance. Another aspect, but not the least, is the realization of micro-segmentation throughout the enterprise that prevents the isolation of sensitive systems such as payment systems, warehouse automation, IoT tools, and cloud workloads. This mitigates the effects of any trade-off and guarantees that their breaches can be confined in time without many operational interruptions.

Another important feature of Zero Trust in a retail setting is vendor access governance. Since the system of third-party suppliers, POS solution vendors, delivery companies, and maintenance contractors is vast, gaining access to third parties is what counts. Zero Trust Network Access (ZTNA) should be used instead of conventional VPN models, which give a user continued access based on the authentication. This will guarantee that the vendors only have the privilege to access the specific systems they are required to at just-in-time, and at the minimum required time only. This model imposes a real-time session monitoring framework, and everything is identity-based, environment-based, and tracing of behaviors. Also, with a growing trend where retailers offload portions of their workloads to cloud-based architectures and API-based commerce applications, it has become critically important to make continuous cloud security posture management, the selective control of secure service identity, and automatic code integrity validation the new standard practice.

The relevance of automation of cyber defense in large-scale retail is the element that will be difficult to overrate. With the scale of distributed users and devices, security orchestration, telemetry correlation, and incident containment automated systems have a critical and important role in reducing mean time to detect and respond to incidents. Integration of extended detection and response (XDR) platforms, real-time threat intelligence, machine learning-based analytics flows allow achieving unified situational awareness that is faster to detect threats and can triage threats faster than achieved manually especially during high seasonal shopping periods. Such automated systems assist the security personnel to work on large volumes of data, minimizing the probability of error by human factor and swift response to the manifested threat.

In the case of the retailers who are planning to adopt Zero Trust, a roadmap must be developed on the basis of the structure and maturity concerning it. The first is the need to make sure that a robust enterprise identity foundation, which has automated life cycle management operations, MFA, and passwordless identifications is created. The Human and machine privilege control is also very vital and should be centrally controlled. High-value systems such as POS infrastructures and payment gateways, e-commerce and warehouse operation technologies should first be targeted in terms of micro-segmentation in investment. Particular attention should be paid to the security of autonomous robotic systems and IoT devices, which will be implemented in fulfillment centers, because all these systems will become elements of real-time realization of logistics processes. Second, it is recommended that the retailers pay attention to utilizing the third-party access control by the means of continually updating the granular ZTNA models, operational session monitoring, and proactive security assessment of vendors. As the number of cloud infrastructures and containerized services are used, security controls must constitute the development pipes in order to provide a secure-by-design implementation of retail

technologies. To detect the abnormalities and prevent malicious actions, the enterprise needs to include continuous monitoring, behavior analysis, and fraud preventing services as well, to diagnose anomalies and stop malicious actions up to the level that can be eliminated. Further, the executive management is supposed to act as a proponent of the Zero Trust implementation, in that it should be a business initiative and not a technical program. The governance setup should include the reporting dimensions and performance measures, proactive work with the regulators at any of the boards levels, so that the Zero Trust endeavors would be coordinated with the general business characteristics, regulatory requirements, and the expectations of the customers regarding the trust.

In the future, Zero Trust will continue to redefine the position of the retail industry as the sphere of autonomic cyber defense and robot-based decisions is expanding. As artificial intelligence evolves, the security teams will be aided with the artificial intelligence, with automatic controls over identity, isolation of suspicious IoT devices to be used, and automatically correction security misconfigured. The growth of robotics application in warehousing and AIs used to manage inventory systems will necessitate high-level machine to machine trust systems, which do not lie down or cause malicious intervention. More so as the retailers roll out new technologies like digital twins, augmented workforce, computer vision-driven loss prevention, and generative AI in the customer engagement, the Zero Trust will have become a root of their new technology implementation on which the latter can be resisted as well as exploited to turn against them.

Zero Trust provides the required platform to amplify the future of operational retail and supply chains and enables organizations to be more creative and, concurrently, resilient, trustworthy, and trusted by customers. By putting the principles of Zero Trust into place across their own digital environment, retailers would be in a position to monitor the constantly-evolving cybersecurity landscape and secure its operations in case of any emergent threat.

REFERENCES

1. Moore et al., The Cost of Cybercrime. Cambridge Univ. Press, 2022.
2. Accenture, “Cybersecurity in Retail & Consumer Goods,” 2023.
3. Bonthu, C. (2025). The role of data governance in strengthening ERP and MDM collaboration. International Journal of Computational and Experimental Science and Engineering. https://ijcesen.com/index.php/ijcesen/article/view/3783
4. Chadha, K. S. (2025). Zero-trust data architecture for multi-hospital research: HIPAA-compliant unification of EHRs, wearable streams, and clinical trial analytics. International Journal of Computational and Experimental Science and Engineering, 12(3), 1–11. https://ijcesen.com/index.php/ijcesen/article/view/3477/987
5. Chavan, A. (2022). Importance of identifying and establishing context boundaries while migrating from monolith to microservices. Journal of Engineering and Applied Sciences Technology, 4, E168. http://doi.org/10.47363/JEAST/2022(4)E168
6. Chavan, A. (2024). Fault-tolerant event-driven systems: Techniques and best practices. Journal of Engineering and Applied Sciences Technology, 6, E167. http://doi.org/10.47363/JEAST/2024(6)E167
7. Cloud Security Alliance, “Zero Trust Advancement Center,” 2023.
8. CrowdStrike, “Global Threat Report,” 2024.
9. Dhanagari, M. R. (2024). MongoDB and data consistency: Bridging the gap between performance and reliability. Journal of Computer Science and Technology Studies, 6(2), 183-198. https://doi.org/10.32996/jcsts.2024.6.2.21
10. Dhanagari, M. R. (2024). Scaling with MongoDB: Solutions for handling big data in real-time. Journal of Computer Science and Technology Studies, 6(5), 246-264. https://doi.org/10.32996/jcsts.2024.6.5.20
11. FAIR Institute, “Cyber Risk Quantification Standard,” 2024.

12. Gartner, "Zero Trust Strategy for Enterprise Security," 2023.
13. Goel, G., & Bhramhabhatt, R. (2024). Dual sourcing strategies. International Journal of Science and Research Archive, 13(2), 2155. https://doi.org/10.30574/ijsra.2024.13.2.2155
14. Google Cloud, "BeyondCorp Enterprise Architecture," 2023.
15. IBM Security, "Cost of a Data Breach Report," 2023.
16. J. Kindervag, "Zero Trust Architecture," Forrester Research, 2010.
17. J. Zhang et al., "AI-Enhanced Identity Analytics," IEEE TIFS, 2023.
18. Karwa, K. (2023). AI-powered career coaching: Evaluating feedback tools for design students. Indian Journal of Economics & Business. https://www.ashwinanokha.com/ijeb-v22-4-2023.php
19. Konneru, N. M. K. (2021). Integrating security into CI/CD pipelines: A DevSecOps approach with SAST, DAST, and SCA tools. International Journal of Science and Research Archive. Retrieved from https://ijsra.net/content/role-notification-scheduling-improving-patient
20. Kumar, A. (2019). The convergence of predictive analytics in driving business intelligence and enhancing DevOps efficiency. International Journal of Computational Engineering and Management, 6(6), 118-142. Retrieved from https://ijcem.in/wp-content/uploads/THE-CONVERGENCE-OF-PREDICTIVE-ANALYTICS-IN-DRIVING-BUSINESS-INTELLIGENCE-AND-ENHANCING-DEVOPS-EFFICIENCY.pdf
21. Malik, G., Brahmbhatt, R., & Prashasti. (2025). AI-driven security and inventory optimization: Automating vulnerability management and demand forecasting in CI/CD-powered retail systems. International Journal of Computational and Experimental Science and Engineering. https://ijcesen.com/index.php/ijcesen/article/view/3855/1153
22. Mandiant, "M-Trends," Google Cloud/Mandiant, 2024.
23. McKinsey, "Securing Digital Commerce at Scale," 2022.
24. Microsoft, "Zero Trust Adoption Report," 2024.
25. MITRE, "ATT&CK Framework," MITRE Corporation, 2023.
26. National Institute of Standards and Technology (NIST), "Zero Trust Architecture," NIST SP 800-207, 2020.
27. Nyati, S. (2018). Transforming telematics in fleet management: Innovations in asset tracking, efficiency, and communication. International Journal of Science and Research (IJSR), 7(10), 1804-1810. Retrieved from https://www.ijsr.net/getabstract.php?paperid=SR24203184230
28. Palo Alto Networks, "State of Zero Trust SOC Automation," 2024.
29. PCI SSC, "Payment Card Industry Data Security Standard v4.0," 2022.
30. Pinnapareddy, N. R. (2025). Serverless computing & function-as-a-service (FaaS) optimization. The American Journal of Engineering and Technology, 7(4), 9. https://doi.org/10.37547/tajet/Volume07Issue04-09
31. Rajgopal, P. R. (2025, August). Secure enterprise browser – A strategic imperative for modern enterprises. International Journal of Computer Applications, 187(33), 53–66. https://doi.org/10.5120/ijca2025925611
32. Raju, R. K. (2017). Dynamic memory inference network for natural language inference. International Journal of Science and Research (IJSR), 6(2). https://www.ijsr.net/archive/v6i2/SR24926091431.pdf
33. SANS Institute, "ICS/OT Cybersecurity Best Practices," 2023.
34. Sardana, J. (2022). The role of notification scheduling in improving patient outcomes. International Journal of Science and Research Archive. Retrieved from https://ijsra.net/content/role-notification-

scheduling-improving-patient

35. Singh, V. (2021). Generative AI in medical diagnostics: Utilizing generative models to create synthetic medical data for training diagnostic algorithms. International Journal of Computer Engineering and Medical Technologies. https://ijcem.in/wp-content/uploads/GENERATIVE-AI-IN-MEDICAL-AGNOSTICS-UTILIZING-GENERATIVE-MODELS-TO-CREATE-SYNTHETIC-MEDICAL-DATA-FOR-TRAINING-DIAGNOSTIC-ALGORITHMS.pdf
36. Singh, V. (2022). Visual question answering using transformer architectures: Applying transformer models to improve performance in VQA tasks. Journal of Artificial Intelligence and Cognitive Computing, 1(E228). https://doi.org/10.47363/JAICC/2022(1)E228
37. Subham, K. (2025). Integrating AI into CRM systems for enhanced customer retention. Journal of Information Systems Engineering and Management. https://www.jisem-journal.com/index.php/journal/article/view/8892
38. Subham, K. (2025). Scalable SaaS implementation governance for enterprise sales operations. International Journal of Computational and Experimental Science and Engineering. https://ijcesen.com/index.php/ijcesen/article/view/3782
39. Sukhadiya, J., Pandya, H., & Singh, V. (2018). Comparison of Image Captioning Methods. INTERNATIONAL JOURNAL OF ENGINEERING DEVELOPMENT AND RESEARCH, 6(4), 43-48. https://rjwave.org/ijedr/papers/IJEDR1804011.pdf
40. Verizon, “2024 Data Breach Investigations Report,” 2024.
41. Z. Yan and X. Liu, “Blockchain-Enabled Supply Chain Security,” IEEE IoT Journal, 2022.