IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Smart and Sustainable Fashion: Integrating Digital Security and Transparency in Sustainable Clothing Supply Chains

Berlin College of Business and Technology

Authored By

1. Maloth Surender Naik

2. Gandham Hima Bindu

3. Bhaskar Teja

Abstract

The fashion industry faces growing scrutiny over its environmental and social impacts while simultaneously experiencing rapid digitalization of its supply chains. Sustainable and circular fashion models are widely promoted, yet consumer skepticism regarding the authenticity of sustainability claims remains high, fueled by information asymmetries and concerns about greenwashing. This paper develops an integrated conceptual framework that links sustainable fashion practices, digital traceability technologies, and cybersecurity mechanisms to explain how these elements jointly influence transparency and consumer trust in clothing supply chains. Drawing on secondary data from academic literature, industry, and ESG reports, technology case studies, and cybersecurity studies, the analysis synthesizes current knowledge on sustainable and circular fashion strategies, digital tracking and authentication tools, and security risks in digital supply networks. The proposed framework argues that secure digital traceability is essential to transform internal sustainability initiatives into credible, externally verifiable information that can reduce information asymmetry and support consumer trust. The paper outlines managerial implications for fashion firms seeking to align sustainability, digital transformation, and security agendas, and identifies directions for future empirical research to test and refine the framework. In particular, managers are advised to prioritise security-by-design, cross-functional governance, and consumer-centric disclosure to build robust, trustworthy, sustainable supply chains.

1 Introduction

The global fashion industry has been criticised for its substantial contribution to climate change, pollution, resource depletion, and labour rights violations. In response, brands and policy-makers have increasingly promoted sustainable and circular approaches that emphasise eco-design, responsible sourcing, recycling, and extended product lifecycles. At the same time, digital technologies have transformed fashion supply chains, enabling real-time tracking, data-driven planning, and closer integration of global production networks. This convergence of sustainability ambitions and digital capabilities has created new

opportunities to monitor and communicate the social and environmental performance of garments across their lifecycle.

Despite these developments, a persistent challenge relates to trust. Many consumers remain unsure whether sustainability and ethical claims are genuine or merely marketing rhetoric. Repeated scandals and accusations of greenwashing have undermined confidence in voluntary corporate disclosures. The complexity and global dispersion of fashion supply chains also make it difficult for stakeholders to independently verify information about origin, working conditions, and environmental impacts. Addressing this credibility gap requires mechanisms that not only collect and manage sustainability-related data but also protect its integrity and present it in an accessible, trustworthy manner.

Digital traceability technologies such as blockchain, RFID, and Internet of Things (IoT) devices offer considerable potential to document the movement and transformation of materials and products throughout the supply chain. When combined with consumer-facing interfaces, these tools can provide detailed information about a garment's history, from raw material extraction to retail. However, the increasing reliance on digital systems also exposes fashion supply chains to cybersecurity risks, including data breaches, tampering with traceability records, and operational disruptions. If not adequately addressed, these risks can compromise transparency initiatives and further erode trust.

Existing research has made substantial progress in understanding sustainable fashion, consumer perceptions of ethical products, the application of digital traceability tools, and cybersecurity in supply chains. Nevertheless, these strands of literature are often treated separately, with relatively little work integrating sustainability, digital transparency, and security within a single conceptual framework. This paper addresses this gap by developing a management-oriented framework that explains how secure digital traceability can support transparency and consumer trust in sustainable fashion supply chains.

The overall aim of the study is to develop an integrated framework showing how digital security technologies can enhance transparency and trust in sustainable fashion supply chains. The specific objectives are to analyse current trends in sustainable and circular fashion markets; to evaluate consumer perceptions of transparency and ethical sourcing; to examine digital technologies that enable traceability and authenticity verification; to assess cybersecurity risks associated with digitalised supply chains; and to design a framework linking sustainability, security, and transparency in a managerial context. The paper addresses the following research questions: How does transparency influence consumer trust in sustainable clothing brands? Which digital technologies are most effective for ensuring traceability and authenticity in fashion supply chains? What cybersecurity risks arise from digitalised supply chains, and how can they be mitigated? How can firms integrate sustainability and digital security into a single strategic framework?

The remainder of the paper is structured as follows. The next section reviews the literature on sustainable and circular fashion, consumer transparency and trust, digital traceability technologies, and cybersecurity in digital supply chains, culminating in a call for an integrated perspective. The methodology section explains the conceptual, secondary-data-based approach adopted. The findings and discussion section synthesises key themes emerging from the literature. The subsequent section presents the proposed conceptual framework and outlines its main propositions. Managerial implications, limitations, and avenues for future research are then discussed, followed by concluding remarks.

2 Literature review

2.1 Sustainable and circular fashion

Sustainable fashion research explores how clothing companies address environmental and social impacts across the product lifecycle. Scholars highlight the industry's traditional reliance on linear "take–make–dispose" models that depend on intensive resource use and generate significant waste and emissions. In response, circular fashion approaches advocate designing garments for longevity, repair, reuse, and recycling, as well as adopting business models based on rental, resale, and refurbishment. These strategies aim to retain the value of materials and products for as long as possible, thereby reducing pressure on natural resources and on waste management systems.

In addition to environmental performance, sustainable fashion encompasses ethical issues such as working conditions, wages, and human rights in global value chains. Regulatory and institutional pressures, including mandatory due diligence rules, extended producer responsibility schemes, and ESG reporting, increasingly require firms to demonstrate responsible practices. Companies have responded with initiatives ranging from sustainable material sourcing and supplier codes of conduct to life-cycle assessment and closed-loop recycling projects. However, critics argue that many efforts remain fragmented, pilot-based, or marketing-oriented, lacking systemic integration into core supply chain processes and governance structures. Only systemic integration embeds sustainability principles into a company's operating model and decision-making at every level, whereas project-level pilots are often one-off or siloed initiatives with limited influence beyond their immediate scope. Some scholars further contend that these initiatives, while visible, may serve primarily as symbolic compliance or public relations strategies rather than leading to substantive change (Brydges et al., 2024; Lupo, 2022). This perspective highlights persistent challenges in translating commitments into verifiable improvements, including limited transparency, inconsistent reporting standards, and the potential for greenwashing. These counterarguments underscore the importance of moving beyond isolated or surface-level measures, raising questions about how sustainability can be operationalized in ways that are both robust and transparent.

2.2 Consumer transparency and trust

Consumer research indicates that transparency is a central determinant of trust in sustainable and ethical products. Because consumers cannot directly observe how garments were produced, there is an inherent information asymmetry between buyers and firms. Theoretical perspectives such as information economics and signaling theory suggest that firms can use signals—such as third-party certifications, eco-labels, corporate reports, and detailed product information—to convey credible evidence of sustainability attributes. Empirical studies show that credible labels and verifiable information can increase perceived trustworthiness and willingness to pay, particularly among consumers who are already concerned about social and environmental issues.

At the same time, the information environment has become increasingly complex. The proliferation of labels, standards, and reporting frameworks can confuse consumers, who may struggle to distinguish between meaningful certifications and weaker marketing claims. Limited time, knowledge, and attention constrain the extent to which consumers engage with detailed sustainability information. Moreover, media coverage of deceptive practices and greenwashing has fostered scepticism, even towards genuinely responsible brands. To reduce the risk of label fatigue and help consumers prioritize among numerous sustainability signals, a simple hierarchy can be established. For example, information can be categorised into three tiers:

(1) Mandatory disclosures, such as government-mandated labels or legally required reporting;

(2) third-party certified claims, including respected eco-labels or independent verifications; and

(3) brand-created or self-declared information, such as proprietary sustainability logos or company-generated statements.

Presenting sustainability data through a transparent hierarchy helps consumers quickly identify the most credible forms of information and make choices that are more informed. For transparency to effectively support trust, information must be reliable, relevant, and presented in a format that consumers can easily understand and use in their decision-making. These points toward the need for traceability and transparency tools that combine technical robustness with user-friendly communication.

2.3 Digital technologies for traceability

Digital technologies are increasingly enabling traceability and authenticity verification in fashion supply chains. Blockchain-based systems have attracted particular interest because they enable multiple stakeholders to record transactions on a tamper-resistant distributed ledger. In the fashion context, blockchain can be used to document the origin of raw materials, processing steps, certifications, and ownership changes along the value chain. Smart contracts can automate aspects of compliance checking and data sharing, potentially reducing opportunities for fraud and enhancing trust among supply chain partners.

Radio-frequency identification (RFID) and IoT devices complement blockchain by providing item level or batch-level identification and real-time tracking capabilities. RFID tags attached to garments or packages can be read automatically at various stages of production and distribution, improving inventory accuracy and supporting anti-counterfeiting measures. IoT sensors may capture environmental and process data, such as temperature or emissions, which can feed into sustainability reporting and quality control. For end consumers, QR codes and digital product passports accessible via smartphones can provide information about the product's journey and characteristics.

While these technologies promise greater visibility and control, they also face significant challenges. Implementation can be costly and complex, especially for small and medium-sized enterprises or highly fragmented supply chains. For example, smaller firms may lack the capital and technical expertise to integrate blockchain or RFID systems, while companies operating across multiple regions may need to align disparate IT infrastructures before adopting shared traceability platforms. A quick stakeholder map highlights where the adoption barriers are most acute: small suppliers often struggle with resource and skill deficits; logistics providers must upgrade legacy systems and ensure interoperability with diverse partners; technology vendors are tasked with supporting multiple standards and customizations; brand owners balance data management across product lines and regions; and certification bodies face the challenge of verifying digital traceability data at scale. Data quality is a critical concern: digital systems can only be as reliable as the accuracy and integrity of the information entered; in practice, errors or inconsistent data entry by supply chain partners can compromise system reliability. Issues of interoperability, standardisation, and governance also arise when multiple organisations must coordinate on shared platforms. For instance, achieving interoperability between different blockchain solutions used by separate supply chain actors can require major investments in data harmonization and the development of common standards. Furthermore, technology-based traceability does not automatically translate into consumer trust unless the information is effectively communicated and perceived as credible.

2.4 Cybersecurity in digital supply chains

The digitalization of supply chains introduces a range of cybersecurity risks that can directly affect traceability and transparency initiatives. Digital supply networks rely on interconnected IT systems, cloud platforms, IoT devices, and data exchanges between firms and external service providers. These connections expand the attack surface for malicious actors who may attempt to steal data, disrupt operations, or manipulate records. Common threats include unauthorized access, data breaches, malware, ransomware, and specific vulnerabilities in poorly secured IoT devices or legacy systems.

A security-first approach is essential for sustainable fashion supply chains, as cybersecurity enables reliable transparency and trust. Only by prioritizing strong digital safeguards from the outset can organisations ensure that sustainability information remains credible and resilient to threats. In the context of sustainable fashion, compromised systems can have serious implications. If attackers can alter traceability records or certification data, the credibility of sustainability claims may be undermined. Disruptions to digital platforms can impede visibility and coordination, affecting product availability and supply chain responsiveness. Information security standards and frameworks emphasise the need to protect the confidentiality, integrity, and availability of data through measures such as access control, encryption, secure software development, monitoring, and incident response planning. However, integrating these cybersecurity practices into sustainability and transparency initiatives is not straightforward and is often neglected in managerial and academic discussions about sustainable fashion.

2.5 Towards an integrated view

The review of existing literature reveals that sustainable fashion, digital traceability, and cybersecurity are typically examined in separate domains. Sustainability studies focus on environmental and social performance, consumer behavior and regulatory pressures, while information systems and operations research concentrate on efficiency, visibility and technological innovation. Cybersecurity research generally prioritizes risk management and resilience without explicitly considering sustainability or consumer trust. A simple unifying logic captures their interplay: sustainability creates the data, traceability moves the data, and cybersecurity secures the data. As a result, there is limited theoretical work that connects how secure digital traceability can transform sustainability practices into credible transparency that supports trust and long-term value creation.

An integrated perspective is needed to understand the interdependencies between these areas. Sustainable fashion practices provide the substantive content—ethical and environmental performance—that needs to be communicated. Digital traceability technologies supply the infrastructure for capturing and sharing relevant information. Cybersecurity mechanisms ensure that this information remains accurate, reliable, and available, thereby underpinning transparency and trust. The next sections of the paper develop a methodology for synthesising these elements, present key themes emerging from the literature, and propose a conceptual framework that links sustainability, digital security, and transparency in fashion supply chains.

3 Methodology

This study adopts a conceptual, secondary-data-based methodology designed to integrate fragmented insights from multiple literatures into a coherent framework. The research design is qualitative and interpretive, focusing on theory building rather than empirical testing. Secondary data sources include peer-reviewed journal articles on sustainable fashion, circular economy, and sustainable supply chain management, as well as studies from information systems, operations management, and cybersecurity. Industry and NGO reports on ESG performance, ethical consumption, and digital supply chain technologies complement the academic literature, together with case studies of technology implementations in fashion and related sectors.

The data collection process involves systematic searching of academic databases and professional sources using keywords related to sustainable fashion, circularity, supply chain transparency, blockchain, RFID, IoT, cybersecurity, and digital supply networks. Inclusion criteria emphasise relevance to the fashion context or to closely analogous consumer industries, conceptual and empirical contributions that address sustainability and digital technologies, and, where possible, recent publications to capture current developments. The selected sources are then reviewed to identify key constructs and relationships relevant to the research aim and questions.

The analysis proceeds through thematic synthesis. Concepts such as sustainability practices, circular models, consumer transparency and trust, digital traceability technologies, cybersecurity controls, and organizational capabilities are coded and grouped into themes. Particular attention is paid to how different sources describe the relationships between visibility, trust, risk, and performance. A comparative analysis of documented cases and models is used to explore similarities and differences in how sustainability, transparency, and security are conceptualized and operationalized. This interpretive process informs the development of an integrated conceptual framework that captures the interconnections between these domains.

This methodological approach acknowledges several important limitations to ensure transparency and clarify the research process's rigor. First, the study relies exclusively on secondary data rather than conducting primary empirical research, such as author-led surveys, interviews, or case studies, so the resulting framework has not yet been directly empirically validated. Second, integrating literature from multiple academic disciplines introduces challenges related to inconsistent terminology and conceptual ambiguity, which may impede the seamless harmonization and coherence of key constructs within the framework. Nevertheless, within the context of this conceptual study—particularly considering the exploratory nature of the research topic and the limited availability of primary empirical evidence—conceptual synthesis using secondary data is a methodologically rigorous choice. This approach enables the consolidation and critical evaluation of diverse evidence, facilitating the construction of a comprehensive, integrative perspective on the subject. Providing a clear and transparent rationale for these methodological choices helps future researchers understand the limitations of the current framework, design empirical studies to further test, and refine its propositions.

4 Findings and discussion

The thematic synthesis yields four main themes that illuminate how sustainability, digital traceability, and cybersecurity interact in fashion supply chains. First, transparency is confirmed as a central determinant of consumer trust in sustainable clothing. Consumers seek information about where and how garments are produced, under what conditions, and with what environmental impacts. However, transparency remains uneven and often difficult to verify, with many brands offering only high-level or selectively curated information. For instance, the controversy surrounding the Higg Index used by several global apparel brands in 2022 illustrates how even well intentioned sustainability disclosures can fall short; despite providing environmental impact scores, brands faced criticism when stakeholders questioned the methodology and struggled to interpret the data meaningfully. Scholars have identified two distinct barriers to effective transparency. Some point to the inherent limitations of transparency itself: not all aspects of sustainability are easily quantifiable or fully reportable, due to commercial sensitivities or data availability issues. These gaps in measurable or disclosed information restrict what can be made transparent in the first place. Separately, other scholars highlight the phenomenon of information fatigue: even when comprehensive data is provided, consumers may lack sufficient context to interpret complex supply chain information or become overwhelmed by an excess of technical details (van der Velden, 2023; Lupo, 2022). Distinguishing between unquantifiable impacts and information overload helps clarify the dual challenges—of incomplete data and difficult-to-process data—that must be addressed with tailored solutions. These counterarguments suggest that transparency alone does not automatically guarantee understanding or trust and must be complemented by effective communication and third-party verification mechanisms. Thus, the persistent gap between consumer expectations and current practice contributes to scepticism and limits the impact of sustainability initiatives on purchasing behaviour.

Second, digital traceability technologies offer practical means to enhance transparency by capturing detailed process and product data across the supply chain. Blockchain can create a shared, immutable record of transactions, RFID and IoT devices can provide item-level tracking and state information, and digital product passports can communicate these details to consumers. Together, these tools have the potential to reduce information asymmetries, support compliance with regulatory requirements, and highlight genuine sustainability efforts. However, significant barriers can impede technology adoption. Integration challenges may arise due to incompatibility with legacy systems and the complexity of coordinating across multiple supply chain partners. The cost of implementation can be prohibitive for small and medium-sized enterprises, particularly when substantial investment in infrastructure and employee training is required. Concerns regarding data quality and standardisation also persist, as the reliability of traceability systems depends on accurate, consistent data entry across all nodes of the supply chain. Furthermore, there may be resistance from supply chain partners who are reluctant to share sensitive information due to competitive concerns or limited technological capacity. These adoption barriers must be addressed to realize the full benefits of digital traceability technologies.

Third, cybersecurity emerges as a critical precondition for reliable transparency. If digital systems are vulnerable to attacks or manipulation, the integrity of traceability information cannot be guaranteed. Recent incidents, such as ransomware attacks on global logistics providers and data breaches affecting fashion and textiles companies, have highlighted how cyber threats can compromise essential supply chain data (Somniac Security, 2025; Just Style, 2024). The financial stakes are considerable: in one recent case, a leading apparel group reportedly suffered operational losses and direct remediation costs exceeding $7 million following a ransomware incident that disrupted material tracking systems for several weeks. For instance, attackers have altered or deleted records related to material origin or certifications, resulting in transparency that is misleading rather than informative. Similarly, cyber incidents can disrupt the availability of information when it is needed, potentially causing operational delays and hindering regulatory

compliance. In addition to undermining consumer trust, such incidents may expose firms to legal liabilities if compromised data leads to the dissemination of false sustainability claims. Furthermore, the reputational damage stemming from high-profile breaches, as observed in recent industry examples, can lessen the perceived value of transparency initiatives and erode relationships with stakeholders, including supply chain partners and certification bodies. Thus, cybersecurity should be viewed not only as a technical or compliance issue but as an essential component of the credibility, effectiveness, and resilience of sustainability and transparency initiatives.

Fourth, organisational and managerial capabilities strongly influence the success of digital sustainability and security initiatives. Implementing secure traceability systems requires collaboration between sustainability, supply chain, IT, and security functions. Governance structures must clarify roles and responsibilities for data management, technology investment, and external communication. Organisational culture should value both environmental and digital responsibility, encouraging continuous learning, risk awareness, and ethical use of data. Without such capabilities, technologies may be implemented in a superficial or fragmented manner, limiting their contribution to transparency and trust.

In summary, the analysis of these themes underscores that sustainable fashion, digital traceability, and cybersecurity are not isolated considerations but rather mutually reinforcing components within a comprehensive strategic framework. Sustainability initiatives drive substantial advances in environmental and social outcomes; digital traceability technologies render these advances transparent and accessible; cybersecurity measures safeguard the credibility of the communicated information; and robust organisational capabilities enable the integration of these domains into unified strategies and clear consumer communications. Building on this synthesis, the following section introduces a conceptual framework to articulate and structure the identified interconnections.

5 Conceptual framework

The conceptual framework developed in this paper can be visualized as a sequential process in which secure digital traceability serves as the pivotal connector between internal sustainability practices and external consumer trust in fashion supply chains. (What's new: the framework unifies three typically siloed literatures, and explicitly elevates cybersecurity as an equal partner with sustainability and digital transparency.)

The framework consists of five distinct yet interrelated components arranged in a logical progression:

(1) Sustainable fashion practices

(2) Digital traceability mechanisms

(3) Cybersecurity and information governance

(4) Transparency and perceived authenticity and

(5) Consumer trust and organizational outcomes.

By structuring these elements in a clear sequence, the framework illustrates how improvements in internal practices, supported by robust digital infrastructure and security measures, can effectively translate into enhanced transparency and consumer confidence.

To provide visual clarity and support for the theoretical structure, Figure 1 below presents a diagram of the conceptual framework. The diagram depicts each component as a stage in a process flow, beginning with sustainable fashion practices and continuing through digital traceability, cybersecurity and information governance, transparency and perceived authenticity, and concluding with consumer trust and organisational outcomes. Arrows between the components indicate the directional influence and

interdependence among these elements. This visual representation reinforces the central argument that secure digital traceability is the critical link joining internal operational improvements to external stakeholder trust in sustainable fashion supply chains.

Conceptual Framework Integrating Sustainability Practices, Digital Traceability, Cybersecurity, and Consumer Trust in Fashion Supply Chains

Sustainable fashion practices include eco-design, responsible material selection, ethical sourcing, improved labour conditions, resource-efficient production, and circular models based on reuse, repair, rental, and recycling. These practices form the substantive basis of sustainability performance. However, in the absence of credible information flows, consumers and stakeholders may not be able to recognise or evaluate these efforts.

Digital traceability mechanisms encompass technologies such as blockchain, RFID, IoT devices, and consumer-facing platforms that capture, store, and communicate data about products and processes. They serve as the infrastructure for recording the life history of garments, from raw material extraction through manufacturing, distribution, retail, and end-of-life pathways. When designed and implemented appropriately, these mechanisms can generate detailed and accessible records that support claims about origin, certifications, and environmental performance.

Cybersecurity and information governance constitute the protective layer that safeguards the integrity, confidentiality, and availability of traceability data. This includes technical measures such as encryption, access control, authentication, and network security, as well as organisational measures such as policies, standards, training, and incident response planning. Without such controls, traceability systems may produce unreliable or manipulable data, undermining the purpose of transparency initiatives.

Transparency and perceived authenticity represent the consumer-facing outcomes of the interaction among sustainability practices, traceability technologies, and security controls. When sustainability efforts are effectively captured and communicated through secure digital systems, consumers can access credible, relevant, and understandable information about garments. This reduces information asymmetry and supports perceptions that the brand's sustainability claims are genuine.

Finally, consumer trust and organisational outcomes refer to the behavioural and strategic consequences of credible transparency. Higher levels of trust are expected to contribute to greater willingness to pay, stronger brand loyalty, positive word of mouth, and reputational resilience. For organisations, these outcomes can translate into competitive advantage, improved stakeholder relationships, and reduced risk of backlash during sustainability controversies.

The framework advances several distinct propositions to inform both future empirical research and managerial practice and clarifies its unique contributions to the literature. The novelty of this framework lies in its explicit and systematic integration of sustainability, digital traceability, and cybersecurity, which have previously been addressed in isolation or only loosely connected in existing models. In contrast to earlier approaches, this framework provides a unified process that brings together these three domains, conceptualising secure digital traceability as the pivotal link transforming internal sustainability initiatives into externally verifiable transparency and, ultimately, consumer trust. This approach extends prior literature by asserting that transparency is not solely a function of adopting digital traceability technologies, but also fundamentally depends on the robustness of cybersecurity measures that protect these systems. Thus, the framework highlights that trust in sustainability claims arises not only from access to information but from its demonstrable reliability and security. By articulating the necessary synergy between sustainability, traceability technologies, and cybersecurity, the framework contributes a novel, cohesive perspective that addresses a notable gap in previous research. This original integration serves as a foundation for empirical

validation and offers practical guidance for organizations seeking to achieve substantive, verifiable, and trustworthy sustainability outcomes.

The conceptual framework developed in this paper can be visualized as a sequential process in which secure digital traceability serves as the pivotal connector between internal sustainability practices and external consumer trust in fashion supply chains. (What's new: the framework unifies three typically siloed literatures, and explicitly elevates cybersecurity as an equal partner with sustainability and digital transparency.) The framework consists of five distinct yet interrelated components arranged in a logical progression: (1) sustainable fashion practices; (2) digital traceability mechanisms; (3) cybersecurity and information governance; (4) transparency and perceived authenticity; and (5) consumer trust and organisational outcomes. By structuring these elements in a clear sequence, the framework illustrates how improvements in internal practices, supported by robust digital infrastructure and security measures, can effectively translate into enhanced transparency and consumer confidence.

Sustainable fashion practices include eco-design, responsible material selection, ethical sourcing, improved labour conditions, resource-efficient production, and circular models based on reuse, repair, rental, and recycling. These practices form the substantive basis of sustainability performance. However, in the absence of credible information flows, consumers and stakeholders may not be able to recognise or evaluate these efforts.

Digital traceability mechanisms encompass technologies such as blockchain, RFID, IoT devices, and consumer-facing platforms that capture, store, and communicate data about products and processes. They serve as the infrastructure for recording the life history of garments, from raw material extraction through manufacturing, distribution, retail, and end-of-life pathways. When designed and implemented appropriately, these mechanisms can generate detailed and accessible records that support claims about origin, certifications, and environmental performance.

Cybersecurity and information governance constitute the protective layer that safeguards the integrity, confidentiality, and availability of traceability data. This includes technical measures such as encryption, access control, authentication, and network security, as well as organisational measures such as policies, standards, training, and incident response planning. Without such controls, traceability systems may produce unreliable or manipulable data, undermining the purpose of transparency initiatives.

Transparency and perceived authenticity represent the consumer-facing outcomes of the interaction among sustainability practices, traceability technologies, and security controls. When sustainability efforts are effectively captured and communicated through secure digital systems, consumers can access credible, relevant, and understandable information about garments. This reduces information asymmetry and supports perceptions that the brand's sustainability claims are genuine.

Finally, consumer trust and organisational outcomes refer to the behavioural and strategic consequences of credible transparency. Higher levels of trust are expected to contribute to greater willingness to pay, stronger brand loyalty, positive word of mouth, and reputational resilience. For organisations, these outcomes can translate into competitive advantage, improved stakeholder relationships, and reduced risk of backlash during sustainability controversies.

The framework advances several distinct propositions to inform both future empirical research and managerial practice and clarifies its unique contributions to the literature. The novelty of this framework lies in its explicit and systematic integration of sustainability, digital traceability, and cybersecurity, which have previously been addressed in isolation or only loosely connected in existing models. In contrast to earlier approaches, this framework provides a unified process that brings together these three domains, conceptualising secure digital traceability as the pivotal link transforming internal sustainability initiatives

into externally verifiable transparency and, ultimately, consumer trust. This approach extends prior literature by asserting that transparency is not solely a function of adopting digital traceability technologies, but also fundamentally depends on the robustness of cybersecurity measures that protect these systems. Thus, the framework highlights that trust in sustainability claims arises not only from access to information but from its demonstrable reliability and security. By articulating the necessary synergy between sustainability, traceability technologies, and cybersecurity, the framework contributes a novel, cohesive perspective that addresses a notable gap in previous research. This original integration serves as a foundation for empirical validation and offers practical guidance for organizations seeking to achieve substantive, verifiable, and trustworthy sustainability outcomes.

6 Managerial implications

The framework offers several implications for managers in sustainable fashion firms. First, sustainability, digital transformation, and cybersecurity should be treated as interconnected strategic priorities rather than separate projects. For example, when selecting a new supplier for recycled materials, firms can simultaneously evaluate the supplier's compliance with digital traceability requirements and cybersecurity protocols during the onboarding process. Decisions about sustainable materials, supplier relationships, and circular business models must be made in parallel with those on data infrastructure, traceability tools, and security investments. Holistic planning can prevent misalignment, duplication of effort, and inconsistent messages to consumers.

Second, managers should carefully select and design traceability technologies that fit the structure, scale, and risk profile of their supply chains. For some firms, a combination of RFID tags and cloud-based databases may be sufficient, while others may benefit from blockchain-based solutions and digital product passports. In all cases, security-by-design principles should be applied, ensuring that data integrity and access control are integrated from the outset rather than added as an afterthought.

Third, effective governance is essential. Firms should establish cross-functional teams involving sustainability, supply chain, IT, cybersecurity, and marketing experts to oversee traceability and transparency initiatives. Clear policies should define who owns sustainability data, who can access and modify it, and how it will be reported to external stakeholders. Collaboration with suppliers and technology partners is also crucial, as traceability and security extend beyond organisational boundaries.

Fourth, communication with consumers must be strategic and user-centric. Providing access to detailed technical data is not enough; information should be presented in accessible formats that highlight the most relevant aspects of sustainability performance and explain how digital systems protect the reliability of that information. However, effective communication strategies require critical attention to both content and delivery channels to maximize consumer engagement and trust. For example, firms could implement interactive QR codes on garment tags, allowing consumers to scan the code with a smartphone and instantly view a curated summary of the product’s sustainability attributes, such as recycled content, fair labor certification, and carbon footprint, supported by digital verification of supply chain data. While such innovations increase information accessibility, firms must also consider the cognitive load and potential information fatigue consumers experience, **and adapt** the depth and complexity of communication to the intended audience. A further practical example is the growing use of digital product passports in the European Union, which compile comprehensive sustainability information and make it available to consumers at the point of sale; yet their effectiveness hinges on the clarity with which complex lifecycle data are translated into actionable insights for diverse consumer segments. Likewise, some brands now employ blockchain-powered mobile apps that trace garment origins and display verifiable environmental and ethical data for each item, though widespread impact depends not only on technological robustness but

also on users' ability to interpret and trust the presented information. Effective strategies go beyond technical transparency by incorporating independent verification, partnerships with credible certification bodies, and transparent disclosure about the limitations of current systems, which together foster trust and facilitate informed consumer decision-making. Overall, critical evaluation and continual refinement of these communication strategies are vital to ensure that consumers receive reliable, meaningful, and usable information rather than an overwhelming surplus of undifferentiated data.

Finally, managers should integrate cyber-risk assessment into broader supply chain and sustainability risk management. Scenario planning and incident response strategies should consider how cyber incidents might affect sustainability-related data and stakeholder perceptions. Proactive investment in security and resilience can protect both operational continuity and reputational capital.

7 Limitations and future research

The conceptual nature of this study entails several limitations, which can be ranked by their likely impact on the validity and robustness of the findings. The most significant limitation concerns the threat to causal inference: the framework is constructed exclusively from secondary sources and interpretive analysis, rather than from primary empirical data gathered directly from fashion companies or consumers. This reliance on pre-existing interpretations increases the risk of embedded biases or omissions and limits the ability to draw direct causal connections between secure digital traceability, transparency, and consumer trust. Consequently, this limitation may affect the generalizability and practical applicability of the framework, as the theoretical relationships proposed have not been empirically tested in real-world industry or consumer contexts. As a result, the findings should be viewed as provisional, and the framework should be considered a theoretically informed model that requires empirical validation and iterative refinement through future research to confirm its relevance and accuracy in practice.

A further limitation relates to conceptual clarity and operationalization challenges. Integrating and harmonizing diverse perspectives from the sustainability, digital traceability, and cybersecurity literature introduces complexity in defining and measuring key constructs, potentially affecting the robustness of the framework in practice.

Next, issues of generalizability must be considered. The framework's explicit focus on the fashion sector provides rich context but may constrain its relevance to industries with different supply chain architectures, stakeholder priorities, or regulatory demands. Sector-specific nuances and industry heterogeneity must therefore be taken into account before direct application elsewhere. Additionally, industry-specific factors such as the pace of technological adoption, organizational readiness, or the maturity of sustainability practices may moderate the efficacy of the proposed model. Nevertheless, the underlying principles connecting sustainability, digital traceability, and cybersecurity could offer a conceptual foundation for other consumer-oriented sectors, albeit with careful adaptation.

Prioritizing these limitations by likely impact is intended to guide future researchers toward the issues that most strongly influence the study's conclusions. To address these limitations, future research should adopt comprehensive empirical approaches, such as large-scale quantitative surveys to probe consumer perceptions of transparency and trust, longitudinal case studies tracking the implementation of digital traceability across different organizational settings, and experimental studies that test how information format influences stakeholder interpretation and behavior. Comparative studies that examine application across sectors and geographies would also enhance the critical assessment of the framework's broader utility. Collectively, these research strategies are necessary to more rigorously assess the framework's adaptability, explanatory power, and practical value beyond the current conceptual boundaries.

To advance the research agenda in this field, future work should pursue several concrete directions. First, quantitative research should test the propositions derived from the proposed framework by employing large-scale consumer surveys and structural equation modeling to measure the relationships between transparency, perceived digital security, and consumer trust across diverse fashion segments. Second, longitudinal qualitative case studies are recommended to document how pioneering fashion companies design, implement, and adapt secure traceability systems over time, with a focus on organizational integration, technological challenges, and multi-stakeholder collaboration. Third, controlled experimental studies should be conducted to assess how different formats and depths of traceability and security information—such as digital product passports, certification displays, or interactive supply chain visualizations—affect consumer understanding, trust, and purchase intentions. Fourth, comparative cross-national and cross-sectoral analyses should examine variations in regulatory environments, cultural expectations, and supply chain configurations to identify external factors that influence the adoption and impact of integrated sustainability and cybersecurity strategies. Finally, action research in collaboration with industry partners could pilot and evaluate new governance models or digital security standards, further bridging academic research and practical implementation in sustainable fashion supply chains.

8 Conclusion

This paper responds to the growing need to understand how digital technologies can support sustainable fashion by developing an integrated framework that connects sustainability practices, digital traceability, and cybersecurity. It argues that digital traceability tools, when combined with robust security and appropriate organisational capabilities, can translate internal sustainability efforts into credible, externally verifiable transparency that reduces information asymmetry and fosters consumer trust. The framework conceptualises secure digital traceability as a bridge between substantive sustainability performance and positive consumer and organisational outcomes.

By synthesising literature from sustainable fashion, information systems, and cybersecurity, the study contributes a cross-disciplinary perspective that is currently underdeveloped in both academic and managerial debates. The proposed framework provides a foundation for future empirical work and practical guidance for fashion firms seeking to build smart, secure, and sustainable supply chains. As the industry continues to evolve under pressure from regulators, consumers, and technological change, integrating digital security and transparency into sustainability strategies will be increasingly vital for maintaining legitimacy, competitiveness, and long-term resilience.

References

- Ellen MacArthur Foundation, 2017. *A new textiles economy: Redesigning fashion's future*. Cowes: Ellen MacArthur Foundation.https://www.frontiersin.org/journals/sustainability/articles/10.3389/frsus.2025.1499273/full
- Jain, S., Pandey, S., and Kaur, R., 2021. Circular economy and sustainability of the clothing and textile industry. *Circular Economy and Sustainability*, 1(1), pp.25–45.https://pmc.ncbi.nlm.nih.gov/articles/PMC8257395/
- Stockholm Resilience Centre, 2020. *A sustainable and resilient circular fashion and textiles industry*. Stockholm: Stockholm Resilience Centre.https://www.stockholmresilience.org/download/18.66e0efc517643c2b8103605/1617805679501/Sustainable%20Textiles%20Synthesis%20Report.pdf

- Brydges, T., Henninger, C.E., and Hanlon, M., 2024. Tensions and duality in developing a circular fashion economy in Europe. *Cambridge Journal of Regions, Economy and Society*, 17(3), pp.577–595.https://academic.oup.com/cjres/article/17/3/577/7721557
- Frontiers in Sustainability, 2025. The Emperor's old clothes: A critical review of circular fashion in gray literature. *Frontiers in Sustainability*, 6, 1499273.
- Lupo, L., 2022. Beyond green promises: How concrete information sparks pride and drives sustainable fashion. *Journal of Sustainable Marketing*, 4(1), pp.45–67.https://luminousinsights.net/articles/JSM-2024-127
- RouSo, 2023. *How transparency builds consumer trust*. Available at: https://s3.fr-par.scw.cloud/rouso/sustainablefashion/how-transparency-builds-consumer-trust.pdf (Accessed: 1 March 2026).https://s3.fr-par.scw.cloud/rouso/sustainablefashion/how-transparency-builds-consumer-trust.pdf
- van der Velden, N., 2023. Redefining transparency in the fashion industry: A study into the digital product passport and consumer behaviour. MSc thesis. Wageningen University & Research.https://edepot.wur.nl/658893
- Nadim, A., 2023. Exploring the potential of blockchain technology within the fashion and textile supply chain with a focus on traceability, transparency, and product authenticity: A systematic review. *Journal of Textile and Apparel Technology and Management*, 13(1), pp.45–68.https://doaj.org/article/5f480f53949f48c9bc4d97311988b8d0
- Khan, M., Pallathadka, H., Adeusi, S. and Tan, K., 2025. Digital transformation in supply chains: Improving resilience and transparency with AI, blockchain, and IoT. *Frontiers in Sustainability*, 6, 1584580.https://www.frontiersin.org/journals/sustainability/articles/10.3389/frsus.2025.1584580/full
- Colab.ws, 2019. The impact of RFID, IIoT, and blockchain technologies on supply chain transparency. *Journal of Manufacturing Technology Management*, 31(3), pp.341–362.https://colab.ws/articles/10.1108%2FJMTM-03-2019-0118
- Saberi, S., Kouhizadeh, M., Sarkis, J. and Shen, L., 2019. The role of blockchain technology in the transition toward sustainable supply chains. *International Journal of Production Economics*, 217, pp.212–226.https://www.sciencedirect.com/science/article/pii/S2667378922000633
- University of Kassel, 2022. Sustainability and blockchain: Defining product provenance and its implications. Kassel: University of Kassel.https://www.uni-kassel.de/fb07/index.php?t=f&f=1438&token=0cc6d9d4ea371969b6cf596e3de643e11ad113da
- Prism Sustainability Directory, 2025. Blockchain traceability for circular fashion supply chains. Available at: https://prism.sustainability-directory.com/scenario/blockchain-traceability-for-circular-fashion-supply-chains/ (Accessed: 1 March 2026).https://prism.sustainability-directory.com/scenario/blockchain-traceability-for-circular-fashion-supply-chains/
- Prism Sustainability Directory, 2025. Blockchain for circular fashion ecosystems. Available at: https://prism.sustainability-directory.com/scenario/blockchain-for-circular-fashion-ecosystems/ (Accessed: 1 March 2026).https://prism.sustainability-directory.com/scenario/blockchain-for-circular-fashion-ecosystems/
- Somniac Security, 2025. Why the fashion and textiles industry faces heightened cybersecurity risks. Available at: https://www.somniacsecurity.com/why-the-fashion-and-textiles-industry-faces-heightened-cyber-security-risks/ (Accessed: 1 March 2026).https://www.somniacsecurity.com/why-the-fashion-and-textiles-industry-faces-heightened-cyber-security-risks/
- Just Style, 2024. Fashion sector digitisation demands greater cybersecurity. *Just Style Magazine*, Issue 16, June. Available at: https://juststyle.nridigital.com/just-

style_magazine_jun23/fashion_sector_digitisation_demands_greater_cybersecurity (Accessed: 1 March 2026).https://juststyle.nridigital.com/just-style_magazine_jun23/fashion_sector_digitisation_demands_greater_cybersecurity

- Anon., 2022. Impact of digital transformation on cybersecurity: Retail and fashion. *International Journal of Novel Research and Development*, 7(3), pp.890–899.https://ijnrd.org/papers/IJNRD2203120.pdf
- The Interline, 2025. The world is primed for digital risk – has fashion kept pace? Available at: https://www.theinterline.com/2025/05/16/the-world-is-primed-for-digital-risk-has-fashion-kept-pace/ (Accessed: 1 March 2026).https://www.theinterline.com/2025/05/16/the-world-is-primed-for-digital-risk-has-fashion-kept-pace/