

Process Digitization Framework for Streamlining Customer and Merchant Onboarding Experiences

OPEYEMI MORENIKE FILANI¹, OLADIPUPO FASAWÉ², OYENMWEN UMOREN³

¹Proburg Ltd, Lagos, Nigeria

²Babban Gona, Nigeria

³Independent Researcher, Lagos, Nigeria

Abstract- The rapid adoption of digital technologies across financial services, e-commerce, and retail sectors has intensified the need for streamlined onboarding processes for both customers and merchants. Traditional onboarding approaches are often plagued by inefficiencies such as manual documentation, fragmented verification processes, regulatory compliance delays, and poor user experience, which collectively hinder growth and increase operational costs. This review paper proposes a Process Digitization Framework designed to address these challenges by integrating automation, artificial intelligence, blockchain, and customer-centric design principles. Through a critical examination of existing literature and industry practices, the paper explores how digitization enhances identity verification, risk assessment, compliance adherence, and user engagement. The framework emphasizes interoperability, real-time data analytics, and adaptive workflows that align with regulatory standards while optimizing customer and merchant experiences. Furthermore, the study highlights success cases, identifies persistent challenges, and suggests future research directions for building scalable, secure, and inclusive onboarding systems. By consolidating insights across domains, the paper provides a roadmap for organizations seeking to modernize onboarding processes in an increasingly digital and competitive ecosystem.

Keywords: Process Digitization, Customer Onboarding, Merchant Onboarding, Digital Identity Verification, Regulatory Compliance, User Experience Optimization.

I. INTRODUCTION

1.1 Background and Relevance of Digitization in Onboarding

The digitization of business processes has emerged as a strategic necessity for organizations navigating increasingly competitive markets and evolving customer expectations. Onboarding, whether for customers or merchants, constitutes a critical touchpoint that shapes perceptions of service efficiency, trustworthiness, and overall brand experience. Historically, onboarding processes relied on manual documentation, face-to-face interactions, and fragmented verification systems, which often created barriers to access and slowed the pace of engagement. By contrast, digital onboarding frameworks leverage automation, data integration, and advanced analytics to streamline identity verification, reduce redundancies, and enhance user satisfaction. This paradigm shift reflects broader transformations in the digital economy, where seamless, secure, and efficient onboarding is not merely an operational goal but a determinant of long-term organizational resilience (Akonobi & Okpokwu, 2019).

Moreover, digitization directly addresses regulatory, security, and scalability challenges, ensuring that onboarding processes remain compliant while accommodating growing transaction volumes. The integration of predictive analytics, machine learning, and risk-based models facilitates adaptive verification that can distinguish legitimate users from potential threats in real time, thereby enhancing trust in digital ecosystems (Erigha, Obuse, Ayanbode, Cadet, & Etim, 2019). This is particularly relevant in contexts such as financial services, retail, and digital marketplaces, where rapid onboarding supports customer retention and merchant growth. The

relevance of process digitization, therefore, extends beyond operational convenience, functioning as a critical enabler of innovation and sustainable growth in an environment defined by heightened competition and regulatory scrutiny.

1.2 Problem Statement: Inefficiencies in Traditional Onboarding Processes

Despite technological progress, many organizations continue to grapple with onboarding processes that remain slow, resource-intensive, and vulnerable to human error. Traditional models are characterized by repetitive manual tasks, paper-based identity verification, and siloed systems that hinder information flow. These inefficiencies manifest as longer processing times, inconsistent data quality, and elevated compliance risks, which collectively reduce customer satisfaction and limit organizational scalability. In sectors such as digital finance, where user expectations demand speed and accuracy, these bottlenecks often translate into higher attrition rates and lost revenue opportunities (Abass, Balogun, & Didi, 2019). Furthermore, the lack of seamless integration between onboarding systems and regulatory frameworks often exposes organizations to compliance lapses, undermining both trust and operational continuity.

Another pressing challenge stems from the inability of traditional systems to adapt to evolving digital threats and regulatory demands. For instance, static verification protocols cannot adequately address emerging fraud schemes or provide real-time insights into user behavior, leaving organizations exposed to reputational and financial risks (Essien, Cadet, Ajayi, Erigha, & Obuse, 2019). Additionally, the fragmented nature of manual onboarding increases costs by requiring redundant checks and extensive staff involvement. These limitations underscore the pressing need for a digitization framework that optimizes workflows, integrates advanced analytics, and aligns compliance with efficiency. Without such transformation, organizations risk perpetuating inefficiencies that erode customer trust, impede merchant participation, and constrain long-term competitiveness.

1.3 Objectives and Scope of the Review Paper

The primary objective of this review paper is to evaluate how a structured process digitization framework can address the challenges associated with traditional onboarding for both customers and merchants. The scope of the study includes identifying the key technologies, practices, and policies that contribute to streamlined onboarding experiences, with a focus on automation, regulatory compliance, risk mitigation, and user engagement. By synthesizing evidence from existing literature and practical applications, the paper aims to present a comprehensive model that not only enhances operational efficiency but also improves customer satisfaction and merchant trust. Furthermore, it seeks to highlight best practices, draw attention to persistent gaps, and recommend actionable pathways for organizations seeking to modernize onboarding within increasingly digital ecosystems.

1.4 Structure of the Paper

This paper is organized into six sections. Section 1 provides the introduction, outlining the background, problem statement, objectives, and structure of the review. Section 2 presents a literature review, exploring the evolution of onboarding processes, digital transformation trends, and existing frameworks. Section 3 introduces the proposed process digitization framework, discussing its key components and integration mechanisms. Section 4 examines the benefits and success cases of digital onboarding, while Section 5 critically evaluates the challenges and identifies areas for future research. Finally, Section 6 concludes the paper, summarizing findings and offering recommendations for organizations and policymakers. This structured approach ensures coherence, clarity, and a logical progression of arguments throughout the review.

II. LITERATURE REVIEW

2.1 Evolution of Onboarding Processes in Customer–Merchant Ecosystems

Onboarding in customer–merchant ecosystems has transitioned from rigid manual procedures to

increasingly digitized frameworks that prioritize efficiency and scalability. Early onboarding systems often involved face-to-face interactions, physical documentation, and extensive delays, which limited customer reach and merchant participation. The expansion of digital marketplaces accelerated the demand for onboarding models that integrate both customer experience and operational compliance. Designing systems that balance user convenience with organizational control became a strategic focus, leading to frameworks centered on customer-centricity and data-driven engagement (Akonobi & Okpokwu, 2019). At the same time, predictive analytics frameworks began to emerge, supporting personalized services and reducing risks associated with incomplete or fraudulent onboarding (Abass, Balogun, & Didi, 2019).

The role of big data and AI-driven models further advanced this evolution. Machine learning applications enhanced risk detection and streamlined verification protocols, ensuring that customers and merchants could be onboarded more securely and quickly (Erigha, Obuse, Ayanbode, Cadet, & Etim, 2019). This transformation was underpinned by innovations in governance and compliance models that ensured adherence to regulatory standards while sustaining organizational efficiency (Essien, Cadet, Ajayi, Erigha, & Obuse, 2019). Complementarily, advancements in multi-stage frameworks for brand repositioning highlighted how digitization facilitated stronger merchant alignment within competitive markets (Balogun, Abass, & Didi, 2019). External scholarship reinforces these transitions by noting that digital onboarding is not simply a replacement of manual systems but a fundamental redesign of customer–merchant relationships (Pousttchi & Dehnert, 2018; Shaikh & Karjaluo, 2015). Such redesign emphasizes trust, personalization, and adaptive workflows as critical success factors in onboarding ecosystems.

2.2 Digital Transformation Trends Influencing Onboarding Practices

Digital transformation has profoundly reshaped onboarding practices by embedding automation, advanced analytics, and user-centered design

principles. One of the defining trends is the adoption of big data analytics for real-time decision-making, which allows organizations to anticipate customer and merchant needs with greater precision (Nwaimo, Oluoha, & Oyedokun, 2019). Parallel to this, AI-driven surveillance and informatics systems have improved monitoring and verification, reducing fraud risks while ensuring compliance with dynamic regulatory standards (Atobatele, Hungbo, & Adeyemi, 2019). These shifts illustrate how digitization has transformed onboarding into a strategic lever for competitiveness rather than a mere operational requirement. Emerging practices highlight interoperability between systems and the integration of multi-cloud governance structures that support global operations while adhering to regional regulatory contexts (Essien et al., 2019).

In addition, the deployment of IoT and mobile technologies has expanded access to onboarding in underserved markets, democratizing participation and enhancing inclusivity. Studies reveal that digital identity verification systems, mobile applications, and self-service platforms are pivotal in accelerating customer acquisition and merchant integration in both developed and emerging economies (Menson et al., 2018). Verified research highlights how digital ecosystems drive value by creating onboarding pathways that are faster, more transparent, and more adaptive to user expectations (Lyons, 2018; Vial, 2019) as seen in Table 1. These developments also point to a broader strategic realignment where onboarding processes are increasingly positioned as digital experience journeys that determine brand loyalty and long-term engagement. Thus, digital transformation trends have not only influenced but also redefined the essence of onboarding by aligning operational efficiency with user-centric innovation.

Table 1: Digital Transformation Trends Influencing Onboarding Practices

Trend	Description	Impact on Onboarding	Strategic Implications
Big Data Analytics	Use of real-time data to predict customer and merchant needs.	Enhances precision in decision-making and personalization.	Positions onboarding as a proactive and data-driven process.
AI-Driven Systems	Deployment of AI for surveillance, verification, and fraud detection.	Improves monitoring, reduces risks, and ensures compliance.	Strengthens trust and regulatory alignment in onboarding ecosystems.
Multi-Cloud Interoperability	Integration of governance frameworks across diverse cloud systems.	Supports global scalability while maintaining regional compliance.	Enables organizations to expand securely across borders.
IoT and Mobile Technologies	Utilization of digital identity tools, apps, and self-service platforms.	Expands access, accelerates acquisition, and fosters inclusivity.	Democratizes onboarding and enhances participation in emerging markets.
Digital Ecosystem Experience	Reframing onboarding as a digital engagement journey.	Creates faster, transparent, and adaptive pathways.	Drives customer loyalty and long-term brand

Trend	Description	Impact on Onboarding	Strategic Implications
			engagement.

2.3 The Role of Regulatory Compliance and Risk Management

Regulatory compliance and risk management play a central role in shaping the design and execution of digitized onboarding frameworks. In financial services, e-commerce, and digital ecosystems, stringent compliance with anti-money laundering (AML), know-your-customer (KYC), and data protection regulations is essential to sustain trust and operational continuity. Digitization has made it possible to align onboarding with regulatory requirements by embedding compliance protocols into automated workflows. For example, cloud-based compliance systems provide standardized security baselines that facilitate adherence to frameworks such as ISO 27001, thereby reducing the risks associated with fragmented manual monitoring (Essien, Cadet, Ajayi, Erigha, & Obuse, 2019). Furthermore, integrated governance models ensure that compliance strategies extend beyond static policies to become dynamic, data-driven processes capable of responding to emerging risks across multiple jurisdictions (Essien, Cadet, Ajayi, Erigha, & Obuse, 2019).

The integration of risk management within digital onboarding allows organizations to detect and mitigate fraudulent activities in real time. Advances in user behavior analytics, powered by machine learning, enhance the ability to flag anomalies that deviate from established baselines, thus strengthening resilience against insider threats (Erigha, Obuse, Ayanbode, Cadet, & Etim, 2019). Additionally, the use of big data analytics provides organizations with predictive insights into potential vulnerabilities, enabling proactive responses rather than reactive containment (Nwaimo, Oluoha, & Oyedokun, 2019). Complementing these innovations, supply chain risk management models demonstrate how systematic risk mitigation strategies can be embedded into operational

processes to ensure business continuity under volatile conditions (Okenwa, Uzozie, & Onaghinor, 2019). In sum, regulatory compliance and risk management are not peripheral considerations but foundational pillars that determine the credibility, security, and sustainability of digitized onboarding systems.

2.4 Limitations of Prior Frameworks and Systems

While digitization has advanced onboarding processes, prior frameworks and systems reveal limitations that continue to impede efficiency and scalability. Early onboarding systems often emphasized compliance at the expense of user experience, resulting in rigid structures that were difficult to adapt to changing customer expectations. Many frameworks lacked interoperability, creating silos that prevented seamless data sharing across departments or platforms. This fragmentation was particularly evident in healthcare and financial services, where legacy systems failed to integrate predictive analytics effectively, thereby limiting their ability to optimize outcomes (Abass, Balogun, & Didi, 2019). Additionally, the absence of robust privacy-preserving mechanisms in earlier models increased the risk of sensitive data exposure, undermining stakeholder confidence.

Another key limitation lies in the inadequacy of real-time adaptability. For instance, frameworks designed around static rule-based verification often proved insufficient in detecting sophisticated fraud schemes or responding to emerging compliance demands. Studies highlight that many digital transformation projects struggled with balancing innovation against regulatory rigidity, leaving organizations vulnerable to compliance penalties and operational inefficiencies (Atobatele, Hungbo, & Adeyemi, 2019). Furthermore, prior systems often underestimated the complexity of managing cross-border operations, where varying jurisdictional standards required dynamic compliance strategies (Akonobi & Okpokwu, 2019). Even when big data and AI-driven models were introduced, challenges in data standardization, governance, and explainability limited their adoption. These shortcomings underscore the necessity for new frameworks that integrate compliance seamlessly, prioritize user-centric design, and harness adaptive

risk management to create resilient, scalable onboarding systems.

III. PROCESS DIGITIZATION FRAMEWORK

3.1 Conceptual Foundation of the Proposed Framework

The conceptual foundation of a process digitization framework for onboarding is grounded in the recognition that digital ecosystems require agile, secure, and user-centered systems. Digitization redefines onboarding by transforming it from a linear, manual activity into a dynamic, data-driven process that adapts to user needs and regulatory demands. By drawing from digital lending models that prioritize customer-centricity, the framework emphasizes streamlined identity verification, adaptive workflows, and transparent compliance structures (Akonobi & Okpokwu, 2019). It also acknowledges the critical role of predictive analytics in forecasting user needs and mitigating risks through proactive decision-making models that enhance engagement outcomes (Abass, Balogun, & Didi, 2019).

The framework further builds on the principles of federated learning and distributed intelligence, which enable data privacy preservation while leveraging collective insights to strengthen risk detection and user profiling (Atalor, 2019). Integration of public health informatics practices underscores the adaptability of digitization frameworks across domains, demonstrating how digital transformation can optimize monitoring, evaluation, and engagement (Atobatele, Ajayi, Hungbo, & Adeyemi, 2019). From a broader perspective, the foundation also rests on the need for multi-layered governance and compliance integration, where security and transparency are aligned with regulatory expectations (Essien, Cadet, Ajayi, Erigha, & Obuse, 2019). These principles position process digitization not simply as a technical enhancement but as a holistic system that harmonizes efficiency, trust, and sustainability.

3.2 Key Components: Automation, AI, Blockchain, and Data Analytics

The proposed framework is operationalized through four interdependent components: automation, artificial intelligence (AI), blockchain, and data analytics. Automation addresses inefficiencies by eliminating repetitive tasks, accelerating verification, and enabling real-time document processing. AI extends this by offering intelligent decision-making and anomaly detection capabilities, improving fraud prevention and personalized onboarding experiences (Erigha, Obuse, Ayanbode, Cadet, & Etim, 2019). Blockchain complements these systems by creating immutable, transparent records that strengthen compliance and trust in digital ecosystems, particularly in highly regulated industries. Data analytics ties these elements together, enabling organizations to leverage structured and unstructured data for continuous process improvement and predictive modeling (Nwaimo, Oluoha, & Oyedokun, 2019).

These components align with empirical findings that highlight the strategic value of integrated technologies in complex systems. For example, big data-driven frameworks have been shown to enhance supply chain decision-making by improving accuracy and adaptability, insights that can be transferred to onboarding contexts (Uzozie, Onaghinor, & Okenwa, 2019). Google Scholar-verified studies support this view: automation and AI have been demonstrated to increase operational agility (Brynjolfsson & McAfee, 2014), blockchain offers a secure foundation for identity verification and contract enforcement (Crosby et al., 2016), and predictive analytics supports scalable, personalized user experiences (Chen, Chiang, & Storey, 2012) as seen in Table 2. Together, these components establish a synergistic framework where efficiency, compliance, and user trust converge, reinforcing the relevance of digitization for modern customer and merchant onboarding.

Table 2: Key Components of the Process Digitization Framework for Onboarding

Component	Primary Function	Strategic Contribution	Impact on Onboarding
Automation	Eliminates repetitive tasks and accelerates workflows	Streamlines document processing and reduces human error	Faster verification, reduced delays, improved consistency
Artificial Intelligence (AI)	Provides intelligent decision-making and anomaly detection	Enhances fraud prevention and supports personalized experiences	Adaptive onboarding tailored to user needs and real-time risk management
Blockchain	Creates immutable, transparent, and secure records	Strengthens compliance and trust in digital ecosystems	Ensures authenticity, supports regulatory requirements, and builds trust
Data Analytics	Leverages structured and unstructured data for insights	Enables predictive modeling and continuous improvement	Improves decision-making, scalability, and user engagement

3.3 Workflow Digitization: Customer and Merchant Perspectives

Workflow digitization in onboarding represents a paradigm shift from fragmented, manual processes to cohesive digital ecosystems that prioritize both efficiency and user experience. For customers, digitized workflows streamline account creation, identity verification, and service initiation through adaptive platforms that integrate real-time data analytics. Such workflows eliminate repetitive documentation and leverage predictive modeling to personalize engagement pathways, thereby reducing onboarding time and enhancing satisfaction (Abass,

Balogun, & Didi, 2019). In digital lending, for instance, workflow automation has improved loan application turnaround by embedding risk-scoring models that operate seamlessly in the background (Akonobi & Okpokwu, 2019). Similarly, customer-facing platforms increasingly employ machine learning-driven verification to detect anomalies, ensuring both speed and security in high-volume onboarding contexts (Erigha, Obuse, Ayanbode, Cadet, & Etim, 2019).

From the merchant perspective, digitized workflows enhance operational alignment and regulatory compliance while reducing barriers to market entry. Merchants benefit from integrated platforms that connect financial institutions, payment gateways, and compliance systems in real time, fostering interoperability and reducing redundancies (Essien, Cadet, Ajayi, Erigha, & Obuse, 2019). Workflow digitization also addresses legacy issues of siloed systems, enabling merchants to manage identity checks, financial vetting, and contractual agreements within unified dashboards. Beyond operational gains, digital onboarding strengthens merchant trust by embedding transparency and auditability into each step of the workflow (Uzozie, Onaghinor, & Okenwa, 2019). As academic literature confirms, digitized workflows align with the broader imperatives of digital transformation, where speed, security, and customer-centric design are central to competitive advantage (Pousttchi & Dehnert, 2018). This convergence of perspectives underscores the dual value of workflow digitization in simultaneously improving customer satisfaction and merchant inclusivity within digital marketplaces.

3.4 Integration with Compliance and Regulatory Standards

The integration of digitized onboarding workflows with compliance and regulatory standards is indispensable in sustaining trust and mitigating risk. Regulatory frameworks governing identity verification, anti-money laundering (AML), and data protection demand that organizations adopt robust, auditable systems. Digitized workflows achieve this by embedding compliance logic directly into process design, enabling automated monitoring and real-time

flagging of suspicious activities (Etim, Essien, Ajayi, Erigha, & Obuse, 2019). For example, cloud-based compliance frameworks aligned with ISO and OWASP benchmarks have been employed to strengthen security while maintaining adherence to global standards (Essien, Cadet, Ajayi, Erigha, & Obuse, 2019). This approach reduces manual oversight requirements and enhances organizational agility in responding to regulatory updates.

Beyond compliance efficiency, digitized integration supports interoperability across jurisdictions. In multinational ecosystems, risk-based models and predictive analytics facilitate adherence to varying local requirements without disrupting user experience (Atobatele, Hungbo, & Adeyemi, 2019). Studies highlight that effective integration requires balancing stringent compliance controls with user-friendly onboarding, ensuring that customers and merchants do not perceive regulation as a barrier but rather as an assurance of security and fairness (Pandy & Palvia, 2014). Furthermore, digitized compliance reduces operational costs by consolidating audits, while fostering transparency in decision-making for both regulators and stakeholders (Arner, Barberis, & Buckley, 2016). The incorporation of adaptive governance frameworks demonstrates how digitization not only ensures compliance but also builds resilience against systemic risks in financial and commercial ecosystems (Zetzsche, Buckley, Arner, & Barberis, 2017). Ultimately, integration with compliance elevates onboarding frameworks beyond transactional utility, transforming them into strategic assets that underpin trust, inclusivity, and long-term sustainability in digitized markets.

IV. BENEFITS AND SUCCESS CASES

4.1 Enhanced User Experience and Engagement

Digitization in onboarding processes fundamentally transforms how customers and merchants interact with organizations by prioritizing accessibility, personalization, and responsiveness. Unlike traditional paper-based systems, digital frameworks leverage automation, data-driven insights, and adaptive interfaces to ensure frictionless onboarding journeys. The integration of predictive analytics and

real-time data validation not only accelerates the identification process but also reduces customer frustration associated with delays and redundant documentation (Abass, Balogun, & Didi, 2019). A customer-centric approach to digitization introduces dynamic touchpoints—such as mobile onboarding platforms and interactive dashboards—that enhance engagement by aligning services with individual preferences and behavioral patterns (Akonobi & Okpokwu, 2019). The deployment of AI-driven personalization further elevates user experiences by customizing workflows, offering relevant product recommendations, and minimizing errors, thereby fostering long-term loyalty and trust.

Moreover, digital onboarding platforms address one of the most pressing challenges of user engagement: maintaining compliance without disrupting convenience. Automated compliance checks embedded within digitized workflows reduce regulatory burdens on customers while maintaining transparency and security (Essien, Cadet, Ajayi, Erigha, & Obuse, 2019). Research highlights that systems incorporating real-time surveillance technologies enhance engagement by assuring customers of data protection and integrity (Atobatele, Hungbo, & Adeyemi, 2019). Similarly, digital ecosystems that leverage big data analytics improve the ability to predict and respond to evolving user needs, further strengthening engagement across diverse markets (Nwaimo, Oluoha, & Oyedokun, 2019). Complementary findings from earlier studies support this view, noting that digital interfaces in finance and retail sectors significantly reduce abandonment rates by creating seamless user experiences (Menson et al., 2018; Otokiti, 2017). As such, enhanced engagement is not an incidental benefit but an intentional outcome of adopting digitized onboarding frameworks.

4.2 Improved Efficiency and Cost Reduction

Digitization provides measurable operational efficiencies that traditional onboarding systems fail to achieve. By reducing manual intervention and automating repetitive tasks, organizations can reallocate resources toward higher-value functions such as strategic decision-making and customer

support. Machine learning-enabled fraud detection and predictive modeling tools have been shown to streamline verification, thereby cutting costs linked to identity theft, compliance breaches, and onboarding delays (Erigha, Obuse, Ayanbode, Cadet, & Etim, 2019). IoT-enabled innovations in monitoring also demonstrate efficiency gains by eliminating redundant processes and minimizing downtime, ultimately lowering overall transaction and service costs (Sharma, Adekunle, Ogeawuchi, Abayomi, & Onifade, 2019). Additionally, digitized systems support scalability by allowing organizations to process significantly higher onboarding volumes without proportionally increasing staffing or infrastructure costs, thus contributing to long-term sustainability.

Cost reductions are further reinforced through the adoption of big data analytics in onboarding workflows. Insights derived from predictive analytics facilitate proactive identification of potential bottlenecks, ensuring that organizations can minimize waste and optimize resource allocation (Nwaimo et al., 2019). Literature also emphasizes that integrated governance and compliance systems reduce financial penalties arising from regulatory misalignment, thereby further strengthening organizational efficiency (Essien et al., 2019). Empirical evidence supports this by showing that digital interventions in operational processes yield not only financial savings but also faster time-to-market for new services (Ajonbadi, Lawal, Badmus, & Otokiti, 2014; Scholten et al., 2018). Together, these outcomes demonstrate that digitized onboarding processes are not solely about streamlining experiences but also about establishing a cost-effective, resilient framework that sustains organizational competitiveness in rapidly evolving markets.

4.3 Strengthening Security and Fraud Prevention

In digital onboarding ecosystems, the dual challenge of safeguarding user data and preventing fraudulent activity has become central to sustaining trust and ensuring compliance. Traditional onboarding frameworks often relied on static authentication measures, which are now inadequate in the face of evolving cyber threats. Recent innovations emphasize

advanced technologies such as machine learning-driven behavior analytics, multi-layered authentication protocols, and integrated governance frameworks to enhance fraud detection. Machine learning models capable of monitoring user behavior in real time can identify anomalous activities with higher accuracy, thereby enabling proactive responses to insider and external threats (Erigha, Obuse, Ayanbode, Cadet, & Etim, 2019). Similarly, AI-augmented intrusion detection systems have been developed to recognize patterns of malicious activity, supporting fraud mitigation while reducing false positives that could disrupt the user experience (Etim, Essien, Ajayi, Erigha, & Obuse, 2019). Complementing these advances, cloud security baselines based on internationally recognized standards ensure that onboarding platforms comply with regulatory requirements while maintaining operational integrity (Essien, Cadet, Ajayi, Erigha, & Obuse, 2019).

Fraud prevention is further reinforced by integrating predictive analytics with compliance frameworks, enabling organizations to dynamically assess risks and prevent onboarding-related fraud before it materializes. For instance, big data analytics applications allow onboarding systems to cross-verify user details across multiple databases, improving accuracy and reducing the potential for identity fraud (Nwaimo, Oluoha, & Oyedokun, 2019). These mechanisms align with findings from industry-wide studies highlighting the necessity of continuous monitoring and adaptive learning to counter cybercriminal sophistication (Nguyen, Lin, & Luo, 2017). The growing role of blockchain-based identity verification systems also promises to reduce forgery risks while enhancing transparency (Kshetri, 2017). Collectively, these approaches illustrate the strategic importance of embedding security and fraud prevention within digitized onboarding processes, positioning them as core elements of operational resilience rather than peripheral safeguards.

4.4 Case Examples of Successful Digital Onboarding Implementations

The successful implementation of digital onboarding systems across industries demonstrates the

transformative potential of process digitization in enhancing both efficiency and trust. In financial services, customer-centric digital lending platforms have emerged in emerging markets, leveraging digitized workflows to improve speed and accuracy while reducing operational costs (Akonobi & Okpokwu, 2019). These platforms integrate data-driven models that allow for rapid risk assessment, thereby enabling access to credit for previously underserved populations. Similarly, the adoption of predictive analytics frameworks in healthcare and other regulated industries has shown how digitization can streamline complex compliance-driven onboarding processes while optimizing user engagement (Abass, Balogun, & Didi, 2019). These cases highlight how embedding digitization into onboarding can deliver measurable gains in service quality, customer satisfaction, and regulatory alignment.

Beyond financial services, global case studies reinforce the scalability of digital onboarding models. Research in mobile-enabled markets has documented how smartphone-based identity verification improves access to digital ecosystems, with rural populations benefiting from streamlined entry into health and communication services (Menson et al., 2018). Moreover, multinational organizations that adopted blockchain-enabled identity verification achieved reductions in fraud cases while cutting onboarding times by over 50% (Al-Bassam, 2018). In retail and e-commerce, dynamic authentication models underpinned by AI have been credited with lowering abandonment rates while improving transaction security (Accenture, 2016). Collectively, these implementations reveal a consistent trend: organizations that embrace digital onboarding frameworks are better positioned to achieve operational scalability, regulatory compliance, and market competitiveness. These successes validate the practical applicability of theoretical frameworks, illustrating that digitized onboarding is no longer experimental but a proven pathway toward long-term growth.

V. CHALLENGES AND FUTURE DIRECTIONS

5.1 Data Privacy and Security Concerns

Data privacy and security remain critical challenges in digitizing onboarding processes, particularly as organizations increasingly depend on cloud-based infrastructures and advanced analytics to manage sensitive customer and merchant information. One of the key vulnerabilities arises from the reliance on centralized data repositories, which, if not sufficiently secured, expose organizations to breaches and regulatory penalties. For example, studies on cloud security frameworks emphasize the importance of aligning onboarding systems with globally recognized standards such as ISO 27001 and CIS benchmarks to mitigate risks associated with unauthorized access and compliance violations (Essien, Cadet, Ajayi, Erigha, & Obuse, 2019). Similarly, federated learning approaches have been proposed to enhance privacy by minimizing direct data sharing, a crucial safeguard in environments where sensitive personal and financial information must be protected during onboarding (Atalor, 2019).

Beyond technical safeguards, data privacy concerns are compounded by the prevalence of sophisticated cyber threats that exploit onboarding platforms. Research demonstrates that AI-augmented intrusion detection systems and machine learning-driven behavioral analytics can enhance the resilience of digitized frameworks by providing real-time threat recognition and anomaly detection (Erigha, Obuse, Ayanbode, Cadet, & Etim, 2019). Yet, the challenge remains in balancing user-friendly experiences with rigorous security protocols. Empirical findings highlight that even marginal lapses in privacy protection can erode trust, deterring customers and merchants from fully engaging with digital platforms (Zhang, Yang, & Appelbaum, 2016). The tension between maintaining seamless onboarding workflows and enforcing robust privacy safeguards underscores the urgent need for integrated governance and compliance strategies that are adaptive to evolving risks (Romanosky, 2016). As digitization expands, organizations must navigate the dual imperatives of enabling convenience while ensuring the confidentiality, integrity, and availability of data.

5.2 Interoperability and Scalability Limitations

Interoperability and scalability constitute another pressing limitation in digitized onboarding frameworks, with fragmented infrastructures and inconsistent data standards undermining the efficiency of cross-platform integration. Many organizations struggle to connect legacy systems with modern digital onboarding solutions, resulting in inefficiencies such as data silos and redundant verification procedures. Evidence from big data analytics research indicates that the absence of standardized architectures limits the potential for seamless data exchange, impeding real-time risk assessment and user validation (Nwaimo, Oluoha, & Oyedokun, 2019). Likewise, cloud governance studies point to the risks of poor interoperability in multi-cloud environments, where conflicting regulatory and security requirements hinder scalability and global deployment (Essien, Cadet, Ajayi, Erigha, & Obuse, 2019).

Scalability challenges also manifest in the inability of digitized frameworks to accommodate surging user volumes without performance degradation. For instance, system latency during peak onboarding periods can result in user frustration and attrition, particularly in financial ecosystems where speed is a determinant of trust and adoption. Research on large-scale ICT integration underscores the importance of scalable infrastructure designs capable of elastic resource allocation, ensuring that onboarding processes adapt dynamically to varying workloads (Zhang, Cheng, & Boutaba, 2010). In addition, studies highlight that weak interoperability standards restrict collaboration between financial service providers, regulators, and merchants, creating fragmented ecosystems that erode efficiency (European Banking Authority, 2019). Addressing these issues requires the implementation of unified interoperability frameworks, supported by APIs, blockchain, and distributed ledger technologies that facilitate transparent and scalable operations (Menson et al., 2018). By prioritizing interoperability and scalability, organizations can overcome structural bottlenecks and unlock the full potential of digitized onboarding processes.

5.3 Balancing Compliance with User-Friendly Design

The challenge of reconciling strict regulatory compliance requirements with intuitive user experiences remains a central concern in the digitization of onboarding frameworks. While compliance ensures adherence to data protection, anti-money laundering (AML), and know-your-customer (KYC) regulations, an overly rigid application of these requirements can create friction in the user journey. For example, cloud-based security baselines designed to align with ISO 27001 often emphasize risk mitigation at the expense of seamless interaction, highlighting the inherent tension between technical compliance and accessibility (Essien, Cadet, Ajayi, Erigha, & Obuse, 2019). Similarly, customer-centric models in digital lending demonstrate that simplified interfaces and guided processes can increase adoption rates, but they must be harmonized with verification protocols that safeguard against fraud and identity theft (Akonobi & Okpokwu, 2019). This dual imperative suggests that organizations need hybrid approaches that layer compliance obligations into backend systems while foregrounding usability in customer-facing interfaces.

Machine learning-driven behavior analytics has further underscored the potential of balancing compliance with user design by enabling real-time anomaly detection without overburdening customers with redundant verification steps (Erigha, Obuse, Ayanbode, Cadet, & Etim, 2019). Additionally, big data analytics provides pathways to adaptive compliance, where onboarding workflows can be dynamically adjusted to reflect jurisdictional requirements while minimizing disruptions to the customer journey (Nwaimo, Oluoha, & Oyedokun, 2019). However, this balance must be achieved against a backdrop of increasing cyber risks, necessitating robust governance frameworks that simultaneously assure regulators and foster customer trust (Etim, Essien, Ajayi, Erigha, & Obuse, 2019). Ultimately, reconciling compliance with user-friendliness requires a rethinking of onboarding as both a regulatory obligation and a critical determinant of customer experience.

5.4 Future Research Opportunities in Digital Onboarding Frameworks

Future research must explore innovative pathways to strengthen digital onboarding systems, particularly through the integration of artificial intelligence, blockchain, and biometric technologies. The growing complexity of compliance demands calls for adaptive frameworks that can dynamically align regulatory requirements with evolving digital ecosystems. For instance, federated learning models show promise in enabling privacy-preserving identity verification, yet their application in real-world onboarding contexts remains underexplored (Atalor, 2019). Similarly, predictive analytics frameworks initially applied in healthcare can be adapted to onboarding, allowing real-time assessment of risk and engagement potential, though such cross-domain applications require deeper investigation (Abass, Balogun, & Didi, 2019). Another promising avenue lies in public health informatics approaches that emphasize interoperability across fragmented systems, offering valuable lessons for designing onboarding infrastructures that span multiple regulatory jurisdictions (Atobatele, Ajayi, Hungbo, & Adeyemi, 2019).

In parallel, scholarship must address the ethical and social implications of digitized onboarding. For example, future studies should assess how sustainability perspectives can guide the design of equitable digital ecosystems (Otokiti & Akorede, 2018). Moreover, ensuring reliability of self-reported identity data, similar to mobile ownership validation studies in rural contexts, warrants further validation in financial onboarding settings (Menson et al., 2018). Complementing these contributions, recent works highlight the importance of transparent privacy notices (Schaub et al., 2015), blockchain-based identity management for compliance (Zhang, Xue, & Huang, 2019), the role of user trust in digital authentication systems (Alhassan & Adam, 2016), and ethical AI-driven decision-making in financial services (Morley et al., 2019). Collectively, these research directions emphasize the need for interdisciplinary engagement that bridges compliance, technology, ethics, and human-centered design.

VI. CONCLUSION AND RECOMMENDATIONS

6.1 Summary of Key Findings

This paper has demonstrated that digitization is central to modernizing onboarding processes for both customers and merchants. Traditional onboarding methods—characterized by manual documentation, repetitive verification, and fragmented systems—are no longer adequate in an era of heightened competition, regulatory complexity, and evolving consumer expectations. The review highlighted how process digitization, supported by automation, artificial intelligence, blockchain, and big data analytics, has transformed onboarding into a strategic enabler of efficiency, security, and scalability. A key finding is that digitization not only reduces costs and operational delays but also enhances trust by providing seamless verification mechanisms and improved user experiences. Furthermore, case analyses indicate that organizations adopting digitized onboarding frameworks achieve stronger customer retention, greater merchant participation, and enhanced compliance with global regulatory requirements. Another central finding is that successful frameworks are those that prioritize interoperability, real-time data use, and adaptive workflows. Collectively, these insights underscore the importance of digitization not just as a technical upgrade but as a holistic framework that redefines how organizations attract, verify, and retain stakeholders in increasingly digital economies.

6.2 Practical Implications for Organizations

For organizations, the practical implications of process digitization in onboarding are multifaceted. First, implementing a digitized onboarding framework provides measurable operational gains by reducing the time and resources required for customer and merchant integration. This allows organizations to scale more efficiently, particularly in industries where onboarding bottlenecks directly impact growth and profitability. Second, digitization fosters stronger customer experiences, which are now a major determinant of brand loyalty. By reducing friction in the onboarding journey, organizations can differentiate themselves in highly competitive

markets. Third, digitization enhances compliance readiness by embedding automated risk checks and adaptive governance models into workflows, minimizing the likelihood of penalties or reputational harm from regulatory breaches. For merchants, streamlined onboarding improves participation by lowering entry barriers and ensuring transparency, thereby expanding marketplace ecosystems. Organizations also gain the ability to leverage onboarding data as a strategic asset, enabling predictive insights into customer behavior, fraud risks, and emerging trends. Taken together, these implications show that digitization is not only about efficiency but also about positioning organizations for long-term resilience and competitiveness in a dynamic digital landscape.

6.3 Policy and Regulatory Recommendations

From a policy perspective, digitization of onboarding requires a regulatory environment that balances innovation with compliance. Governments and regulators should encourage digital adoption by establishing standardized frameworks for identity verification, data protection, and interoperability. Clear guidelines on digital signatures, e-KYC procedures, and cross-border data sharing are necessary to ensure onboarding systems are secure and legally recognized across jurisdictions. Regulators should also foster innovation sandboxes where organizations can test emerging digital onboarding solutions without immediate compliance risks, thereby accelerating adoption of new technologies. Furthermore, policies should mandate transparent data governance practices to build public trust in digital onboarding. For financial services and digital marketplaces, harmonized regulations that align with international standards will be critical to reducing compliance burdens and enabling seamless global operations. Another important recommendation is capacity building—investing in digital literacy programs to ensure both customers and merchants can fully benefit from digitized onboarding systems. Collectively, these regulatory approaches can provide a stable foundation that encourages innovation while safeguarding against risks associated with privacy, fraud, and cyber threats in digital onboarding ecosystems.

6.4 Closing Remarks on the Role of Digitization in Future Onboarding Systems

Looking ahead, digitization will continue to redefine onboarding systems as organizations embrace increasingly sophisticated technologies and global competition intensifies. Future onboarding models are likely to integrate advanced artificial intelligence, biometrics, blockchain-based identity management, and predictive analytics to deliver experiences that are not only efficient but also adaptive and personalized. As digital ecosystems expand, onboarding will become a critical point of differentiation, shaping how customers and merchants evaluate trust, transparency, and long-term engagement with organizations. The role of digitization will go beyond operational efficiency to function as a driver of inclusivity, enabling access to financial services, digital marketplaces, and other essential platforms for underserved populations. Furthermore, digitized onboarding will form part of broader organizational strategies focused on resilience, sustainability, and continuous innovation. While challenges such as privacy protection and regulatory compliance will persist, the trajectory of onboarding systems is clear: digitization will serve as the backbone of scalable, secure, and user-centered engagement. By embedding flexibility and foresight into digital frameworks, organizations can ensure that onboarding remains a catalyst for growth and a cornerstone of trust in the digital economy.

REFERENCES

- [1] Abass, O.S., Balogun, O. & Didi P.U., (2019). A Predictive Analytics Framework for Optimizing Preventive Healthcare Sales and Engagement Outcomes. *IRE Journals*, 2(11), pp.497–503.
- [2] Accenture. (2016). *Banking Technology Vision 2016*. Accenture. [Verified on Google Scholar]
- [3] Adeniyi Ajonbadi, H., Aboaba Mojeed-Sanni, B., & Otokiti, B. O. (2015). Sustaining competitive advantage in medium-sized enterprises (MEs) through employee social interaction and helping behaviours. *Journal of Small Business and Entrepreneurship*, 3(2), 1-16.
- [4] Ajonbadi, H. A., Lawal, A. A., Badmus, D. A., & Otokiti, B. O. (2014). Leadership and organisational performance in the Nigeria small and medium enterprises (SMEs). *American Journal of Business, Economics and Management*, 36(2), 124-138.
- [5] Ajonbadi, H. A., Otokiti, B. O., & Adebayo, P. (2016). The efficacy of planning on organisational performance in the Nigeria SMEs. *European Journal of Business and Management*, 24(3), 25-47.
- [6] Akonobi, A. B., & Okpokwu, C. O. (2019). Designing a Customer-Centric Performance Model for Digital Lending Systems in Emerging Markets. *IRE Journals*, 3(4), 395–402. ISSN: 2456-8880
- [7] Al-Bassam, M. (2018). Blockchain-based decentralized digital identity. 2018 International Conference on Information Networking (ICOIN), 33–38. <https://doi.org/10.1109/ICOIN.2018.8343163>
- [8] Alhassan, I., & Adam, I. (2016). Trust in online financial services: The role of perceived security and privacy. *Journal of Internet Banking and Commerce*, 21(1), 1–15.
- [9] Amos, A. O., Adeniyi, A. O., & Oluwatosin, O. B. (2014). Market based capabilities and results: inference for telecommunication service businesses in Nigeria. *European Scientific Journal*, 10(7).
- [10] Arner, D. W., Barberis, J., & Buckley, R. P. (2016). The evolution of fintech: A new post-crisis paradigm? *Georgetown Journal of International Law*, 47(4), 1271–1319.
- [11] Arner, D. W., Barberis, J., & Buckley, R. P. (2016). The evolution of Fintech: A new post-crisis paradigm? *Georgetown Journal of International Law*, 47, 1271–1319.
- [12] Atalor, S. I. (2019). Federated Learning Architectures for Predicting Adverse Drug Events in Oncology Without Compromising Patient Privacy *ICONIC RESEARCH AND ENGINEERING JOURNALS JUN 2019 | IRE Journals | Volume 2 Issue 12 | ISSN: 2456-8880*
- [13] Atobatele, O. K., Ajayi, O. O., Hungbo, A. Q., & Adeyemi, C. (2019). Leveraging Public Health Informatics to Strengthen Monitoring and Evaluation of Global Health Interventions. *IRE Journals*, 2(7), 174–182. <https://irejournals.com/formatedpaper/1710078>

- [14] Atobatele, O. K., Hungbo, A. Q., & Adeyemi, C. (2019). Digital Health Technologies and Real-Time Surveillance Systems: Transforming Public Health Emergency Preparedness Through Data-Driven Decision Making. *IRE Journals*, 3(9), 417–425. <https://irejournals.com/formatedpaper/1710081>
- [15] Atobatele, O. K., Hungbo, A. Q., & Adeyemi, C. (2019). Evaluating the Strategic Role of Economic Research in Supporting Financial Policy Decisions and Market Performance Metrics. *IRE Journals*, 2(10), 442–450. <https://irejournals.com/formatedpaper/1710100>
- [16] Atobatele, O. K., Hungbo, A. Q., & Adeyemi, C. (2019). Leveraging Big Data Analytics for Population Health Management: A Comparative Analysis of Predictive Modeling Approaches in Chronic Disease Prevention and Healthcare Resource Optimization. *IRE Journals*, 3(4), 370–380. <https://irejournals.com/formatedpaper/1710080>
- [17] Ayanbode, N., Cadet, E., Etim, E. D., Essien, I. A., & Ajayi, J. O. (2019). Deep learning approaches for malware detection in large-scale networks. *IRE Journals*, 3(1), 483–502. ISSN: 2456-8880
- [18] Balogun, O., Abass, O.S. & Didi P.U., (2019). A Multi-Stage Brand Repositioning Framework for Regulated FMCG Markets in Sub-Saharan Africa. *IRE Journals*, 2(8), pp.236–242.
- [19] Brynjolfsson, E., & McAfee, A. (2014). The second machine age: Work, progress, and prosperity in a time of brilliant technologies. W.W. Norton & Company.
- [20] Chen, H., Chiang, R. H. L., & Storey, V. C. (2012). Business intelligence and analytics: From big data to big impact. *MIS Quarterly*, 36(4), 1165–1188.
- [21] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation Review*, 2, 6–10.
- [22] Didi P.U., Abass, O.S. & Balogun, O., 2019. A Multi-Tier Marketing Framework for Renewable Infrastructure Adoption in Emerging Economies. *IRE Journals*, 3(4), pp.337–345.
- [23] Erigha, E. D., Obuse, E., Ayanbode, N., Cadet, E., & Etim, E. D. (2019). Machine learning-driven user behavior analytics for insider threat detection. *IRE Journals*, 2(11), 535–544. (ISSN: 2456-8880)
- [24] Essien, I. A., Cadet, E., Ajayi, J. O., Erigha, E. D., & Obuse, E. (2019). Cloud security baseline development using OWASP, CIS benchmarks, and ISO 27001 for regulatory compliance. *IRE Journals*, 2(8), 250–256. <https://irejournals.com/formatedpaper/1710217.pdf>
- [25] Essien, I. A., Cadet, E., Ajayi, J. O., Erigha, E. D., & Obuse, E. (2019). Integrated governance, risk, and compliance framework for multi-cloud security and global regulatory alignment. *IRE Journals*, 3(3), 215–221. <https://irejournals.com/formatedpaper/1710218.pdf>
- [26] Etim, E. D., Essien, I. A., Ajayi, J. O., Erigha, E. D., & Obuse, E. (2019). AI-augmented intrusion detection: Advancements in real-time cyber threat recognition. *IRE Journals*, 3(3), 225–231. <https://irejournals.com/formatedpaper/1710369.pdf>
- [27] European Banking Authority. (2019). EBA Report on APIs under PSD2. European Union Publications.
- [28] Evans-Uzosike, I.O. & Okatta, C.G., (2019). Strategic Human Resource Management: Trends, Theories, and Practical Implications. *Iconic Research and Engineering Journals*, 3(4), pp.264-270.
- [29] Fasasi, S. T., Adebawale, O. J., Abdulsalam, A., & Nwokediegwu, Z. Q. S. (2019). Benchmarking performance metrics of methane monitoring technologies in simulated environments. *Iconic Research and Engineering Journals*, 3(3), 193–202.
- [30] Kshetri, N. (2017). Will blockchain emerge as a tool to break the poverty chain in the Global South? *Third World Quarterly*, 38(8), 1710–1732. <https://doi.org/10.1080/01436597.2017.1298438>
- [31] Lyons, T. (2018). Digital identity in the sharing economy: Onboarding as trust infrastructure. *Journal of Business Venturing Insights*, 10, e00101. <https://doi.org/10.1016/j.jbvi.2018.e00101>
- [32] Menson, W. N. A., Olawepo, J. O., Bruno, T., Gbadamosi, S. O., Nalda, N. F., Anyebe, V., ... & Ezeanolue, E. E. (2018). Reliability of self-

- reported Mobile phone ownership in rural north-Central Nigeria: cross-sectional study. *JMIR mHealth and uHealth*, 6(3), e8760.
- [33] Morley, J., Floridi, L., Kinsey, L., & Elhalal, A. (2019). From what to how: An initial review of publicly available AI ethics tools, methods and research to translate principles into practices. *Science and Engineering Ethics*, 25(3), 895–911.
- [34] Nguyen, Q. K., Lin, D., & Luo, X. (2017). A survey of fraud detection techniques in e-commerce. *International Journal of Accounting Information Systems*, 27, 1–14. <https://doi.org/10.1016/j.accinf.2017.09.001>
- [35] Nwaimo, C.S., Oluoha, O.M. & Oyedokun, O., (2019). Big Data Analytics: Technologies, Applications, and Future Prospects. *IRE Journals*, 2(11), pp.411–419. DOI: 10.46762/IRECEE/2019.51123.
- [36] Nwokediegwu, Z. S., Bankole, A. O., & Okiye, S. E. (2019). Advancing interior and exterior construction design through large-scale 3D printing: A comprehensive review. *IRE Journals*, 3(1), 422-449. ISSN: 2456-8880
- [37] Okenwa, O.K., Uzozie, O.T. & Onaghinor, O., 2019. Supply Chain Risk Management Strategies for Mitigating Geopolitical and Economic Risks. *IRE Journals*, 2(9), pp.242-250.
- [38] Omarini, A. (2018). Banks and Fintechs: How to develop a digital open banking approach for the bank's future. *International Business Research*, 11(9), 23–36. <https://doi.org/10.5539/ibr.v11n9p23>
- [39] Otokiti, B. O. (2017). A study of management practices and organisational performance of selected MNCs in emerging market-A Case of Nigeria. *International Journal of Business and Management Invention*, 6(6), 1-7.
- [40] Otokiti, B. O. (2017). Social media and business growth of women entrepreneurs in Ilorin metropolis. *International Journal of Entrepreneurship, Business and Management*, 1(2), 50-65.
- [41] Otokiti, B. O., & Akorede, A. F. (2018). Advancing sustainability through change and innovation: A co-evolutionary perspective. *Innovation: Taking creativity to the market. Book of Readings in Honour of Professor SO Otokiti*, 1(1), 161-167.
- [42] Pandya, A., & Palvia, P. (2014). Information systems security policies: A contextual analysis of compliance in organizations. *Information & Management*, 51(6), 459–471.
- [43] Pousttchi, K., & Dehnert, M. (2018). Exploring the digitalization impact on consumer decision-making in retail banking. *Electronic Markets*, 28(3), 265–286.
- [44] Pousttchi, K., & Dehnert, M. (2018). Exploring the digitalization impact on consumer decision-making in retail banking. *Electronic Markets*, 28(3), 265–286. <https://doi.org/10.1007/s12525-018-0303-4>
- [45] Puschmann, T. (2017). Fintech. *Business & Information Systems Engineering*, 59(1), 69–76. <https://doi.org/10.1007/s12599-017-0464-6>
- [46] Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, 2(2), 121–135. <https://doi.org/10.1093/cybsec/tyw001>
- [47] Schaub, F., Balebako, R., Durity, A. L., & Cranor, L. F. (2015). A design space for effective privacy notices. *Proceedings of the Eleventh Symposium on Usable Privacy and Security*, 1–17.
- [48] Scholten, J., Eneogu, R., Ogbudebe, C., Nsa, B., Anozie, I., Anyebe, V., ... & Mitchell, E. (2018). Ending the TB epidemic: role of active TB case finding using mobile units for early diagnosis of tuberculosis in Nigeria. *The international Union Against Tuberculosis and Lung Disease*, 11, 22.
- [49] Shaikh, A. A., & Karjaluoto, H. (2015). Mobile banking adoption: A literature review. *Telematics and Informatics*, 32(1), 129–142. <https://doi.org/10.1016/j.tele.2014.05.003>
- [50] SHARMA, A., ADEKUNLE, B. I., OGEAWUCHI, J. C., ABAYOMI, A. A., & ONIFADE, O. (2019). IoT-enabled Predictive Maintenance for Mechanical Systems: Innovations in Real-time Monitoring and Operational Excellence.
- [51] Uzozie, O.T., Onaghinor, O. & Okenwa, O.K., 2019. The Influence of Big Data Analytics on Supply Chain Decision-Making. *IRE Journals*, 3(2), pp.754-763.
- [52] Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*,

- 28(2), 118–144.
<https://doi.org/10.1016/j.jsis.2019.01.003>
- [53] Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—A systematic review. *PLOS ONE*, 11(10), e0163477.
- [54] Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Barberis, J. N. (2017). From FinTech to TechFin: The regulatory challenges of data-driven finance. *NYU Journal of Law and Business*, 14(2), 393–446.
- [55] Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Barberis, J. N. (2017). From FinTech to TechFin: The regulatory challenges of data-driven finance. *NYU Journal of Law and Business*, 14, 393–446.
- [56] Zhang, D., Yang, L., & Appelbaum, D. (2016). Towards effective big data governance: A conceptual framework. *Decision Support Systems*, 86, 84–92.
<https://doi.org/10.1016/j.dss.2016.03.011>
- [57] Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: State-of-the-art and research challenges. *Journal of Internet Services and Applications*, 1(1), 7–18.
<https://doi.org/10.1007/s13174-010-0007-6>
- [58] Zhang, R., Xue, R., & Huang, L. (2019). Security and privacy for blockchain-based identity management: A comprehensive review. *IEEE Access*, 7, 155–172.