A Systematic Appraisal of Multi-Factor Authentication Mechanisms for Cloud-Based E-Commerce Platforms and Their Effect on Data Protection

Manisha Khadka, Lumbini Science and Technology University, Department of Computer Science, Peace Street, Lumbini, Nepal.

Abstract

Cloud-based e-commerce platforms rely on trust, robustness, and seamless user experiences to facilitate secure transactions across global marketplaces. Multi-factor authentication (MFA) represents a cornerstone technology designed to reinforce login and authorization procedures. The combination of something the user knows, has, or is, integrated into a layered protection scheme, strengthens the security posture of cloud-based systems while aiming to preserve customer convenience. Numerous organizations deploy MFA strategies to thwart an expanding array of cyber threats, including credential theft, data breaches, and phishing attacks, which have seen increased sophistication in modern e-commerce environments. A methodical appraisal of these authentication mechanisms illustrates how various deployment models provide distinctive benefits and limitations when safeguarding sensitive transaction data. Growing complexities arise when cloud-based infrastructures expand and incorporate diverse application programming interfaces (APIs), software-as-a-service (SaaS) solutions, and mobile endpoints. MFA demands systematic considerations regarding network scalability, user experience design, and the balancing act between rigorous security standards and platform accessibility. Cryptographic methods, biometrics, one-time passwords (OTPs), physical tokens, and adaptive risk-based systems convey diverse levels of resilience against intruders seeking to compromise e-commerce transactions. The interplay between user adoption and stringent enforcement mechanisms poses a challenge in maximizing the efficacy of MFA while ensuring minimal friction in the purchasing journey. The present work delivers a systematic analysis of multi-factor authentication mechanisms for cloud-based e-commerce platforms by examining prominent methods and their interplay with system architecture. This discussion dissects the intricacies of how various MFA schemes affect data protection, offering insights into the areas where continuous development, innovative solutions, and robust governance frameworks can provide enhanced resilience. Technical considerations and operational strategies that facilitate secure e-commerce operations in a cloud-centric era are illuminated. Potential avenues for future research are also identified, reflecting an urgent need to continuously adapt to evolving threats. This research underscores how strategic MFA deployment can significantly elevate confidence among users, safeguard e-commerce transactions, and prevent damaging security breaches.

1. Introduction

Cloud-based e-commerce ecosystems store and process significant amounts of confidential user and transactional data. Rapid globalization of online marketplaces and easy accessibility of web-based or mobile shopping interfaces drive higher transaction volumes, thereby attracting malicious actors who seek to exploit weak points in authentication and data management layers [1], [2]. Internet connectivity and distributed architectures expand the attack surface, exposing system components to an ever-increasing variety of intrusion tactics that go beyond simple brute force. Denial-of-service attempts, coordinated phishing campaigns, and advanced persistent threats may target data repositories and

authentication credentials. Multi-factor authentication (MFA) has emerged as a fundamental safeguard to mitigate these threats, yet variations in organizational architecture, compliance obligations, and user preferences mandate customized MFA solutions.

E-commerce data often includes financial information, personal identification details, and commercial secrets such as inventory statistics or supply chain records. Data exfiltration incidents, where criminals gain unauthorized access and retrieve sensitive records, can devastate public trust, inflict financial loss, and undermine the stability of online marketplaces. The fluid nature of e-commerce, where user sessions are active around the clock, presents continuous opportunities for intrusion attempts. Automated scripts and bots frequently test login credentials gathered from previous data leaks, seeking credentials that remain unchanged or poorly secured. Even basic security fundamentals, like password complexity, prove insufficient in restraining these evolving tactics.

Implementation of data protection measures within cloud-based infrastructures poses distinct challenges, since these platforms rely on remote servers, virtualized services, and multi-tenant architectures. Conventional perimeter-based defenses may struggle to adequately protect geographically dispersed resources, especially when traffic passes through multiple network segments. E-commerce portals often rely on dynamic scaling practices to handle fluctuating transaction loads, calling for equally agile security controls that can adapt to workload demands. MFA counters unauthorized logins through additional security layers, yet deploying it at scale calls for careful orchestration of cryptographic keys, identity provisioning procedures, and real-time risk analyses.

Biometric technologies, physical hardware tokens, and software-based one-time passwords exist as prominent MFA methods designed to supplement knowledge-based credentials. Such mechanisms create more stringent barriers to entry, limiting the success rates of password-guessing attempts or phishing attacks. However, misconfigurations and usability constraints might negate potential benefits. Cloud-based e-commerce must integrate MFA that aligns with the risk profiles of transactions, taking into account varying levels of user expertise, device diversity, and regulatory mandates. Organizations that implement robust solutions often face challenges related to customer friction, user adoption, and cost overheads. User frustrations in inputting extra codes or scanning fingerprints may lead to cart abandonment or decreased satisfaction, while data regulators impose stiff penalties for compliance failures.

Fine-grained balance between strong security and user experience remains the central tension. MFA solutions designed for B2B transactions might differ substantially from those suited for general consumer transactions. Specialized hardware tokens and robust cryptographic modules might be more acceptable in closed enterprise environments than in consumer-facing e-commerce. As more data migrates to decentralized storage nodes or serverless architectures, comprehensive assessments of how MFA interacts with the cloud e-commerce lifecycle become critical. The ensuing sections detail the architecture of MFA, evaluate various factors that inform its effectiveness, and contextualize how these solutions protect the integrity of data within cloud-based e-commerce ecosystems.

2. Core Principles and Implementation of Multi-Factor Authentication

Multi-factor authentication involves the convergence of multiple, independent checks that confirm user identity before granting system access. Knowledge (passwords, PINs), possession (hardware tokens, mobile devices), and inherence (biometrics) categories form the traditional foundation of MFA. By

compelling users to fulfill at least two of these factor types, organizations reduce reliance on single points of failure. The rationale lies in the assumption that compromising multiple barriers is more difficult than guessing or stealing one set of credentials.

Contemporary MFA deployments often utilize time-based one-time passwords (TOTPs), which generate ephemeral numeric codes that expire quickly, thereby minimizing interception risks. Such passcodes may be delivered via text messages or specialized mobile applications. Short Message Service (SMS)-based MFA enjoys widespread adoption but faces vulnerabilities when threat actors exploit SIM-swapping or intercepting SMS messages. Authenticator apps using cryptographic underpinnings and offline generation of one-time codes significantly reduce these dangers. Physical security tokens, such as Universal 2nd Factor (U2F) devices, confirm user presence and possession of a dedicated hardware unit. These solutions offer minimal friction once configured, although distribution and cost considerations might discourage their use in large-scale consumer contexts.

Biometric authentication methods, leveraging unique physiological or behavioral attributes, remove the need for memorized secrets and can decrease reliance on external tokens. Fingerprint scanners, facial recognition algorithms, and voice or iris matching constitute varied biometric modalities. These approaches hinge on the accurate capture and matching of a user's biometric data, a process vulnerable to false positives if sensor quality or matching algorithms are inadequate. Biometric data breaches prompt concerns about irreversibility, since once an individual's fingerprint template is compromised, it cannot be revoked or reset in the same manner as a password.

Adaptive or risk-based MFA introduces contextual checks to supplement or replace traditional methods, examining metadata like geolocation, device type, user behavior patterns, or transaction amounts. If a user's login attempt originates from a previously used device at a familiar location, the system may forgo extra verification steps to limit friction. Conversely, access from new locations or devices triggers more comprehensive checks, potentially requiring an additional passcode or biometric scan. This dynamic approach reduces disruption for legitimate users while heightening scrutiny in suspicious circumstances. Careful calibration of risk thresholds is essential to avoid overlooked risks or overly aggressive lockouts.

Implementation of MFA within cloud-based e-commerce architectures hinges on identity and access management (IAM) frameworks [3]. These systems provision, monitor, and deprovision user identities across distributed software components. When integrated with cloud services, IAM orchestration must handle ephemeral containers, serverless functions, and continuous delivery pipelines that define cloud-native workflows. Automated triggers can enforce MFA whenever high-risk operations occur, such as administrative console logins or changes to critical data sets. This targeted approach provides more granular security than blanket MFA across all interactions.

Cryptographic key management extends beyond the immediate scope of passwords or biometric templates. Token-based authentication often uses public key infrastructure (PKI) to validate digital signatures. Cloud-based e-commerce merchants must either manage key infrastructure themselves or rely on third-party certificate providers. The key lifecycle—generation, rotation, revocation, and archival—demands thorough oversight, especially when multiple tokens or certificates protect the same environment. Any oversight in this process might weaken the efficacy of MFA, giving rise to session hijacking or privilege escalation tactics.

Integration with modern e-commerce platforms includes careful consideration of software interfaces that handle checkout processes, user dashboards, and administrative functions. The adoption of representational state transfer (REST) and GraphQL APIs allows decoupled services to communicate seamlessly, which means IAM solutions must align with these architectural styles [4]. MFA can be triggered automatically at discrete points in an API-based workflow, disallowing further progression without the necessary verification. e-Commerce platforms operating on multi-cloud or hybrid-cloud models require consistent policy enforcement across providers, ensuring that users encounter unified security measures wherever they engage with the system [5].

Testing and auditing remain integral to verifying whether MFA has been configured properly across an e-commerce environment. Penetration testers typically attempt to bypass MFA methods through social engineering, credential stuffing, or exploitation of misconfigured servers. Detection of vulnerabilities or flaws leads to adjustments in policy thresholds, user education campaigns, or advanced technical measures such as hardware security modules (HSMs). Logging and monitoring systems gather audit trails of authentication attempts, which serve as a valuable data source for incident response and forensic analysis. Comprehensive MFA metrics—adoption rates, false positives, user lockouts, and average login times—provide critical insights for iterative improvement.

3. Analysis of Diverse MFA Mechanisms for Cloud-Based E-Commerce

Hardware tokens supply a tangible factor of possession, offering robust security and typically requiring an authorized user to insert or tap a specialized device to complete the login process. Physical tokens often incorporate cryptographic challenge-response protocols that limit susceptibility to phishing or replay attacks. Costs and logistics can complicate adoption when e-commerce organizations aim to distribute tokens to a worldwide customer base. Token malfunction or loss might prompt user inconvenience, which could discourage consistent use of this MFA method.

Software-based OTPs provide a flexible solution that can be deployed to mobile phones, tablets, and desktops. Users install authenticator applications that generate six- or eight-digit codes synchronized with an authentication server, based on time or event triggers. These apps circumvent SMS-based vulnerabilities, yet remain subject to device-level threats if malware infiltrates the user's phone or if the phone operating system is compromised. E-commerce sites that incorporate these OTP systems can reduce friction by allowing offline generation of codes without requiring cellular connectivity, which benefits global shoppers who rely on different network infrastructures.

Biometric authentication in the e-commerce cloud environment often leverages device-native sensors. Smartphones commonly include fingerprint readers or facial recognition systems that can grant user access without re-entering passwords. Cloud-based platforms integrate with native biometric libraries, passing along proof of successful authentication. While this method is simple to adopt if hardware supports it, the authentication strength depends on the device's security model. In certain cases, attackers might exploit software vulnerabilities to bypass biometric checks. The irreversibility of biometric data necessitates robust privacy protections and encryption of stored templates.

Risk-based or adaptive MFA tailors authentication prompts according to real-time analysis of user actions. An e-commerce user logging in from a recognized device may experience a simplified process, while a request from an unrecognized IP range triggers additional checks. This approach lowers friction during typical usage yet raises alertness for unusual patterns. Data analytics engines ingest behavioral

information, factoring in velocity checks (unusually rapid attempts), geolocation mismatches, and correlation with known malicious IP addresses. Implementation demands thorough calibrations to avoid either excessive false positives or missed anomalies. Transparency of these mechanisms can be a double-edged sword: if attackers learn how risk analysis is performed, they may tailor their tactics to circumvent triggers.

Push notifications have gained traction as an accessible MFA method. Users with a registered mobile application receive a prompt to approve or deny a login attempt. This real-time verification step gives them direct control over suspicious activity. However, the reliance on stable internet connectivity and correct push configuration might render this method ineffective if notifications fail to arrive. Also, “push fatigue” arises when frequent login attempts cause users to absentmindedly approve notifications without reviewing their legitimacy. Proper rate-limiting, user education, and context-based prompts are necessary to mitigate this risk.

Serverless architectures, common in cloud-native e-commerce, complicate MFA integration by distributing application logic across numerous small functions. The ephemeral nature of these functions limits the window for persistent sessions. MFA solutions therefore have to orchestrate session tokens or short-lived credentials that are valid across multiple function invocations. Improperly configured serverless workflows might skip essential authentication steps under certain workflows, highlighting the importance of robust design. Audits of serverless code repositories and automation of security checks in continuous integration/continuous deployment pipelines are crucial to ensure consistent MFA enforcement.

Single sign-on (SSO) often intersects with MFA in enterprise e-commerce scenarios. Users who manage multiple business relationships or partner portals rely on centralized identity providers that handle a single set of authentication credentials. Layering MFA onto SSO can streamline user access across multiple resources. This synergy demands adherence to standards such as Security Assertion Markup Language (SAML) or OpenID Connect, which pass authentication claims between providers and service components. The security of this chain is only as strong as the weakest link, so enforcing MFA at the identity provider level is critical.

Cryptographic hardware modules like HSMs or Trusted Platform Modules (TPMs) offer tamper-resistant key storage that can manage high-volume cryptographic operations. By offloading certain encryption or signing tasks to these secure modules, e-commerce platforms reduce exposure of private keys. Integration with MFA occurs when hardware modules store secrets required for challenge-response authentication. System architects must weigh costs and complexity against the security benefits of hardware-level protections. Large e-commerce vendors, processing thousands of transactions per second, often find these modules indispensable for advanced key management at scale.

Reviewing these various mechanisms reveals a spectrum of security strengths and usability considerations. Achieving the desired level of data protection in a global, cloud-based e-commerce environment frequently requires a combination of these methods to address a wide array of potential vulnerabilities. Fine-tuned risk-based approaches, strong cryptographic underpinnings, and hardware-level protections each contribute to a multi-layer security model that can withstand targeted attacks.

4. Impact of MFA on Data Protection in E-Commerce

Data protection rests on the premise that only authorized individuals can access, manipulate, or transfer sensitive records. MFA significantly reduces the likelihood of unauthorized logins, thus mitigating risk of account takeover, fraudulent transactions, or large-scale data theft. As transaction volumes grow, the window for malicious activities can also increase, so robust authentication is essential to containing that risk. MFA raises the threshold attackers must surpass to compromise an account. Even if credentials are leaked or phished, the adversary must bypass a secondary check, which may involve access to a user's smartphone, biometric feature, or hardware token [6].

In the context of regulatory compliance, strong authentication mechanisms help e-commerce platforms align with requirements for data protection [7], [8]. Governments and industry bodies often impose guidelines that recommend or mandate MFA for high-risk activities. Comprehensive MFA usage also assists in meeting standards associated with payment processing and identity verification [9]. Adopting MFA can insulate a business from reputational harm in the aftermath of a breach, by demonstrating that robust safeguards were in place. Customers and partners tend to trust platforms that openly prioritize their data protection, improving brand loyalty and fostering long-term business relationships [10].

Implementing MFA in a cloud context affects data protection by extending defenses beyond conventional perimeter security. Cloud-based systems rely on shared responsibility models, where the provider ensures the underlying infrastructure's security while the client remains accountable for access controls and data configurations. Even if the cloud provider implements certain security features, the e-commerce merchant retains control over how users authenticate. MFA steps into this gap by serving as a user-centric barrier that counters most infiltration attempts. Sensitive information stored in cloud databases is less vulnerable to misuses if the gateway to these resources demands multiple validation factors [11].

Encryption strategies that accompany MFA reinforce data protection. Many advanced tokens or authenticator apps rely on cryptographic protocols that securely transmit and verify login data. By employing robust encryption, e-commerce platforms ensure that even if an adversary intercepts the communication channel, the data gained is insufficient to recreate or replay an authorization request. End-to-end encryption fortifies communication flows, while token-specific keys limit the potential impact of compromise to a singular factor rather than the entire authentication chain.

Biometric-based MFA exerts a notable influence on data protection by eliminating vulnerabilities tied to shared or re-used passwords. Stolen passwords from third-party breaches are commonly tested on multiple platforms. If an e-commerce merchant relies solely on passwords, the likelihood of successful credential stuffing increases. Biometrics inhibit such attacks because malicious actors cannot reuse a stolen password to pass a biometric check. However, breach of biometric databases can be catastrophic due to the permanent nature of biometric traits. Protective measures, such as hashing or template encryption, become essential for limiting the fallout of compromised biometric data.

Adaptive MFA contributes to data security by bolstering authentication only when necessary. This strategy expedites legitimate user logins but rigidly guards high-value transactions or logins from suspicious networks. Adaptive policies can deny or flag transactions that deviate from normal usage patterns, preventing suspicious orders from going through until the user provides secondary confirmation. Balancing operational requirements with data privacy regulations calls for well-designed workflows that guard sensitive data without infringing on user autonomy.

Usage of MFA also generates valuable authentication logs that feed into security information and event management (SIEM) systems. Each successful or failed attempt produces a record that can be correlated with other events for anomaly detection. Security teams can analyze these logs to derive insights about compromised accounts, brute force attempts, or repeated suspicious access patterns. In turn, these insights guide refinements to the MFA policy, adjusting threshold or reauthentication prompts. Through iterative improvements, e-commerce platforms can continually strengthen their posture and detect emerging vulnerabilities.

Proactive testing remains the keystone of ensuring that MFA genuinely fortifies data protection. Ethical hacking engagements and red-team exercises reveal overlooked dependencies and configuration oversights. If a single sign-on portal omits MFA for specific API endpoints, attackers could exploit this opening to bypass the entire system. Thorough code reviews and architectural scans confirm that no backdoors or misconfigurations exist in production. When these measures are supplemented by security awareness training for staff and end users, the combined outcome creates a culture where MFA is actively respected and operationally effective.

5. Discussion and Future Outlook

Cloud-based e-commerce stands at the juncture of massive scalability, distributed operations, and continuous innovation in digital retail strategies. MFA emerges as a defensive bulwark for organizations seeking to protect data assets in light of growing threats and sophisticated adversaries. The mosaic of authentication methods—hardware tokens, software-based OTPs, biometrics, risk-based systems, and push notifications—enables merchants to tailor solutions that address the nuances of their user base. Implementing a comprehensive approach to MFA, wherein multiple solutions function in tandem, can create a holistic barrier capable of withstanding varied intrusions.

Balancing user experience against security strictness remains a persistent challenge. MFA inevitably introduces additional steps for authentication, which may cause friction. Excessively onerous protocols can dissuade customers, hurting revenue and discouraging adoption. Light-touch solutions, however, may fail to deter determined attackers. Adaptive MFA attempts to strike an equilibrium, aligning the level of verification with real-time risk signals. Dynamic adjustment allows e-commerce providers to maintain usability in typical scenarios and deploy rigorous checks only when anomalies surface. This approach ensures minimal disruption while offering robust protection.

Rapid evolution of artificial intelligence and machine learning may accelerate the sophistication of risk-based authentication. Behavioral biometrics, analyzing user typing cadence or mouse movements, can operate transparently in the background. Integration of advanced AI-driven threat intelligence could enable real-time feedback loops that identify unusual shifts in user behavior. Biometrics relying on facial or voice recognition might incorporate deep-learning algorithms that refine matching accuracy over time. Although these techniques promise increased security, they raise critical ethical questions about data privacy, potential biases, and long-term storage of sensitive personal attributes.

Hardware security modules may become more prevalent in e-commerce cloud deployments, delivering advanced cryptographic management for large-scale operations. Greater adoption of quantum-resistant algorithms is also conceivable, to prepare for future computational threats that might break current asymmetric encryption standards. Incorporation of user-managed keys or secure enclaves, where portions of the authentication flow run within isolated environments, could grant individuals more direct

control over their data and reduce the centralization of risk. Emergence of technologies like decentralized identities or blockchain-based verification might further shape the next generation of MFA [12].

E-commerce portals that cater to millions of users across different jurisdictions must take into account regulatory frameworks that encourage or mandate MFA. Data protection laws and cybersecurity guidelines may evolve toward stronger requirements for multi-factor mechanisms, particularly in payment processing or healthcare-related transactions [13]. Platforms without robust authentication risk legal penalties, reputational damage, and potential dissolution of business relationships. Conversely, e-commerce providers that incorporate flexible, user-friendly MFA solutions may gain competitive advantages by signaling a strong security commitment.

Inconsistent user adoption surfaces as a problematic area. While employees in enterprise environments may be obligated to use hardware tokens, the general consumer audience can be more resistant to extra login steps. Gamification strategies, user education campaigns, and offering multiple MFA choices can mitigate frustration. Some organizations rely on incentives, such as loyalty points, to motivate users to enable MFA voluntarily. Gradual transitions, where optional MFA eventually becomes mandatory, help manage user expectations and reduce abandonment rates.

Further research into integrative security analytics platforms might yield consolidated dashboards that empower security teams to unify identity management, encryption, and MFA processes within the same interface. Automated policy enforcement could extend from identity provisioning to session termination, ensuring that no user can bypass essential multi-factor checks. Because cloud-based e-commerce typically involves ephemeral workloads and containerized infrastructure, the capacity to continuously monitor and adapt to changes is fundamental. Rolling out new features without simultaneously updating MFA rules can create security blind spots.

Exploration of usability under challenging conditions, such as areas with limited network bandwidth or high latency, constitutes another dimension of future progress. If customers in remote regions cannot promptly receive SMS messages or push notifications, e-commerce platforms must support alternative methods. Offline codes, printable backup keys, and robust device-based tokens might bridge these gaps. Comprehensive support for global user bases remains a necessity, as e-commerce markets continue to expand beyond developed regions into territories with constrained connectivity [14].

Emphasis on emergent threats and infiltration strategies is vital for continued improvement. Attackers might refine sophisticated social engineering tactics aimed at tricking users into sharing OTPs or accepting push notifications for fraudulent requests. Zero-day vulnerabilities in mobile operating systems or cloud orchestration platforms could bypass entire layers of defense [15]. E-commerce security must proactively review these risks and design layered responses that combine technical controls with human awareness. Multi-layered authentication only works if it is accompanied by robust procedures for verifying user identities offline, quarantining suspicious access attempts, and continuously updating security policies.

Concluding reflections underscore that multi-factor authentication stands as a foundational element of data protection strategies for cloud-based e-commerce platforms. By layering factors drawn from different dimensions—knowledge, possession, and inherence—organizations elevate the difficulty for potential attackers. Data protection outcomes depend on thorough integration with identity

management, cryptographic key handling, and continual auditing. Adaptations of MFA for the evolving technology landscape will be indispensable, ensuring that user credentials remain secure in the face of emerging adversarial capabilities [16], [17]. The ensuing progress in AI-driven risk assessment, hardware security modules, and flexible deployment models signals that MFA will continue to evolve as the gateway to secure e-commerce experiences. In a future marked by global scale, diverse device usage, and sophisticated threats, vigilant attention to MFA design and deployment will remain a pivotal determinant of data integrity and consumer trust.

References

[1] V. R. Kebande, F. M. Awaysheh, R. A. Ikuesan, S. A. Alawadi, and M. D. Alshehri, "A Blockchain-based Multi-Factor authentication model for a cloud-enabled Internet of vehicles," *Sensors (Basel)*, vol. 21, no. 18, p. 6018, Sep. 2021.

[2] J. Zhang and H. Mao, "Multi-factor identity authentication protocol and indoor physical exercise identity recognition in wireless sensor network," *Environ. Technol. Innov.*, vol. 23, no. 101671, p. 101671, Aug. 2021.

[3] A. Velayutham, "Mitigating Security Threats in Service Function Chaining: A Study on Attack Vectors and Solutions for Enhancing NFV and SDN-Based Network Architectures," *International Journal of Information and Cybersecurity*, vol. 4, no. 1, pp. 19–34, 2020.

[4] C. Jacomme and S. Kremer, "An extensive formal analysis of multi-factor authentication protocols," *ACM Trans. Priv. Secur.*, vol. 24, no. 2, pp. 1–34, May 2021.

[5] D. Kaul, "Optimizing Resource Allocation in Multi-Cloud Environments with Artificial Intelligence: Balancing Cost, Performance, and Security," *Journal of Big-Data Analytics and Cloud Computing*, vol. 4, no. 5, pp. 26–50, 2019.

[6] J. Williamson and K. Curran, "The role of multi-factor authentication for modern day security," *semicond. sci. and inf. n.a.*, vol. 3, no. 1, pp. 16–23, May 2021.

[7] S. V. Bhaskaran, "Enterprise Data Architectures into a Unified and Secure Platform: Strategies for Redundancy Mitigation and Optimized Access Governance," *International Journal of Advanced Cybersecurity Systems, Technologies, and Applications*, vol. 3, no. 10, pp. 1–15, 2019.

[8] C. K. Ayo, C. M. Mac-Eze, A. A. Adebiyi, A. Oni, J. O. Okesola, and I. Odun-Ayo, "Developing a multi-factor authentication-based cardless electronic payment system," *IOP Conf. Ser. Earth Environ. Sci.*, vol. 665, no. 1, p. 012009, Mar. 2021.

[9] R. Khurana, "Fraud Detection in eCommerce Payment Systems: The Role of Predictive AI in Real-Time Transaction Security and Risk Management," *International Journal of Applied Machine Learning and Computational Intelligence*, vol. 10, no. 6, pp. 1–32, 2020.

[10] A. S. Cvetković, V. Radojčić, and S. Adamović, "Multi-factor authentication for the Internet of Things," *ZB. RAD. UNIV. SINERGIJA*, vol. 22, no. 7, Mar. 2021.

[11] S. Shekhar, "An In-Depth Analysis of Intelligent Data Migration Strategies from Oracle Relational Databases to Hadoop Ecosystems: Opportunities and Challenges," *International Journal of Applied Machine Learning and Computational Intelligence*, vol. 10, no. 2, pp. 1–24, 2020.

[12] B. O. ALSaleem and A. I. Alshoshan, "Multi-Factor Authentication to Systems Login," in *2021 National Computing Colleges Conference (NCCC)*, Taif, Saudi Arabia, 2021.

[13] S. Shekhar, "Integrating Data from Geographically Diverse Non-SAP Systems into SAP HANA: Implementation of Master Data Management, Reporting, and Forecasting Model," *Emerging Trends in Machine Intelligence and Big Data*, vol. 10, no. 3, pp. 1–12, 2018.

[14] M. Sain, O. Normurodov, C. Hong, and K. L. Hui, "A survey on the security in cyber physical system with multi-factor authentication," in *2021 23rd International Conference on Advanced Communication Technology (ICACT)*, PyeongChang, Korea (South), 2021.

[15] A. Velayutham, “Architectural Strategies for Implementing and Automating Service Function Chaining (SFC) in Multi-Cloud Environments,” *Applied Research in Artificial Intelligence and Cloud Computing*, vol. 3, no. 1, pp. 36–51, 2020.

[16] L. Loffi, C. M. Westphall, L. D. Grüdtner, and C. B. Westphall, “Mutual authentication with multi-factor in IoT-Fog-Cloud environment,” *J. Netw. Comput. Appl.*, vol. 176, no. 102932, p. 102932, Feb. 2021.

[17] G. L. Moepi and T. E. Mathonsi, “Multi-factor authentication method for online banking services in South Africa,” in *2021 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, Cape Town, South Africa, 2021.