Journal of Current Science and Research Review
Volume 2 Issue 2, December (2024) ISSN: 2961-0869
https://jcsrr.org/index.php/jcsrr ORIGINAL ARTICLE

OPEN ACCESS

Enhancing Digital Security: How Identity Verification Mitigates E-Commerce Fraud

Swapnil Patil[1], Vikesh Dudhankar[2], Pradyumna Shukla[3]

1 IEEE USA
2 Kennesaw State University USA
3 IEEE USA

Abstract
The exponential growth of e-commerce has revolutionized how transactions are conducted, offering unprecedented convenience and global reach. However, this transformation has also attracted sophisticated cyber threats, including identity theft, account takeovers, and phishing scams, resulting in significant financial and reputational losses. Mobile identity verification has emerged as a pivotal solution, leveraging technologies such as biometrics, multi-factor authentication (MFA), and AI-driven analytics to combat fraud effectively. This paper explores the role of mobile identity verification in enhancing the security of digital transactions in e-commerce. Through a review of recent advancements, case studies, and data analysis, we demonstrate how mobile verification systems reduce fraud, foster consumer trust, and streamline compliance with regulatory frameworks. Despite its efficacy, challenges such as usability concerns, cost barriers, and technical vulnerabilities persist. We propose innovative solutions, including the integration of blockchain technology and advanced behavioral analytics, to address these limitations and outline future research directions for optimizing transaction security in the digital age.

Keywords: Mobile identity verification, e-commerce fraud, digital transaction security, biometrics, multi-factor authentication, AI in fraud prevention, blockchain technology

Introduction

1.1 Background
The e-commerce landscape has undergone a meteoric rise, reshaping global trade by offering unparalleled convenience and accessibility. With this growth, however, has come an alarming increase in fraudulent activities, jeopardizing the trust and financial security of consumers and businesses alike. Fraudulent schemes, ranging from phishing attacks to account takeovers, exploit vulnerabilities in digital ecosystems, often targeting inadequate or outdated identity verification mechanisms.
The advent of mobile identity verification marks a significant leap forward in addressing these challenges. By leveraging mobile technologies such as biometrics and multi-factor authentication (MFA), these systems provide robust, real-time authentication, effectively mitigating the risk of fraud while enhancing user convenience. Furthermore, advancements in AI and machine learning have enabled predictive capabilities, allowing businesses to preempt potential threats with unprecedented accuracy.

1.2 Problem Statement
Despite these advancements, fraud remains a persistent issue in the e-commerce sector. Traditional identity verification methods, such as passwords and knowledge-based authentication, have proven inadequate against increasingly sophisticated cyber threats. The need for secure, scalable, and user-friendly verification solutions has never been more critical.

1.3 Objectives
This study aims to explore the pivotal role of mobile identity verification in reducing fraud within e-commerce. It evaluates the impact of mobile verification technologies on transaction security, assesses their adoption and usability, and proposes innovative solutions to address existing challenges.

1.4 Research Questions
- How does mobile identity verification reduce fraud in e-commerce transactions?
- What are the critical technologies underpinning effective mobile verification systems?
- What barriers impede the widespread adoption of mobile identity verification?

This paper provides an in-depth analysis of these questions, offering actionable insights to enhance the security and reliability of digital transactions.

2. Literature Review

The literature review explores the current landscape of e-commerce fraud, examines traditional and modern identity verification systems, delves into the technologies underpinning mobile identity verification, and discusses the regulatory framework influencing their implementation.

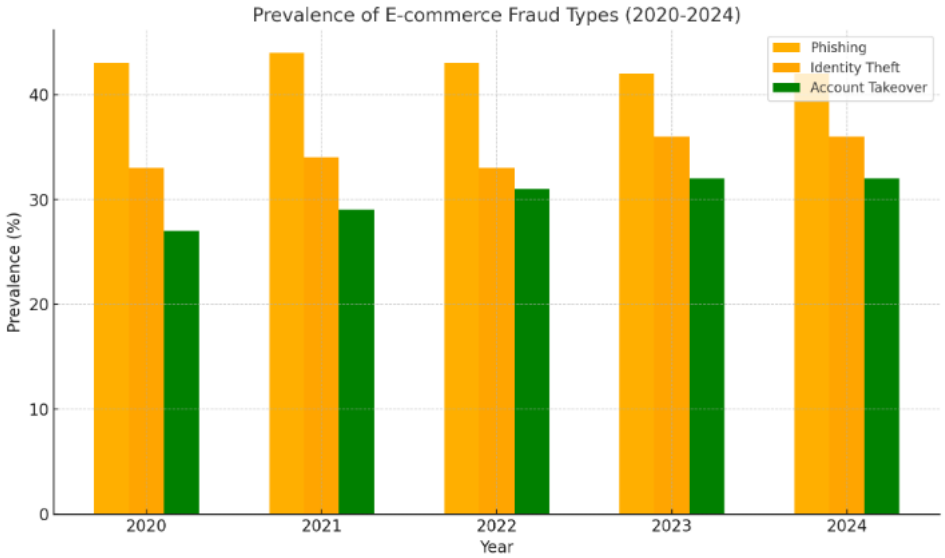
2.1 Overview of E-Commerce Fraud Trends

E-commerce has revolutionized global commerce, but it has also created fertile ground for cybercriminal activities. Fraud in online transactions continues to rise, with tactics evolving in sophistication. Common fraud types include:

- **Phishing**: Deceptive practices to steal sensitive information via fake websites or emails.
- **Identity Theft**: Unauthorized use of personal information to access accounts or make purchases.
- **Account Takeovers**: Breaching existing user accounts to carry out fraudulent activities.

Table 1: Common E-Commerce Fraud Types and Their Impact

Fraud Type	Description	Impact on E-Commerce	Examples
Phishing	Fake communications to obtain credentials	Loss of consumer trust, financial losses	Fake emails, cloned websites
Identity Theft	Misuse of personal data	High cost of reimbursement, lawsuits	Stolen social security numbers
Account Takeover	Unauthorized account access	Compromised data, chargebacks	Breached passwords via malware



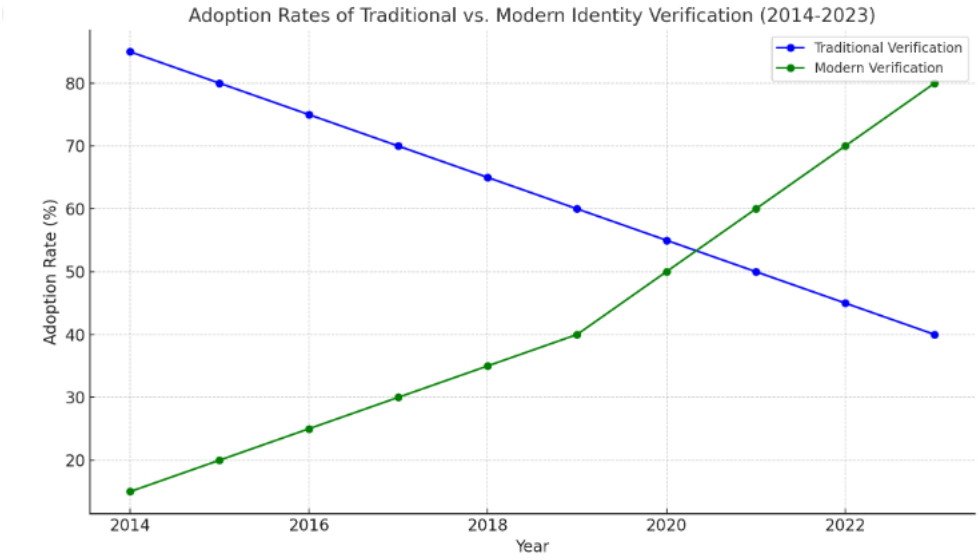
2.2 Evolution of Identity Verification Systems

Identity verification has evolved from traditional methods, such as username-password combinations, to more sophisticated digital solutions:

1. **Legacy Systems**
   - Relied on static identifiers such as passwords and PINs.
   - Vulnerable to brute force attacks, phishing, and data breaches.
2. **Modern Advancements**
   - Incorporation of multi-factor authentication (MFA), combining knowledge (passwords), possession (OTP via SMS), and inherence (biometrics).
   - Deployment of tokenized authentication and device recognition technologies.

Table 2: Comparison of Legacy vs. Modern Identity Verification Systems

Aspect	Legacy Systems	Modern Systems
Security Level	Low	High
Usability	Moderate	High
Resistance to Cybercrime	Low	High
Integration with Devices	Limited	Seamless across devices



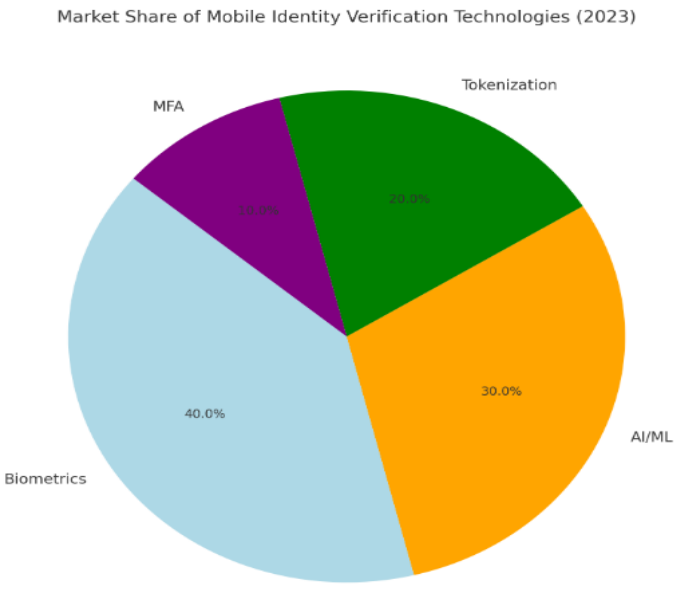
2.3 Mobile Identity Verification Technologies

Mobile devices have become integral to secure identity verification processes. Key technologies enabling this transformation include:

1. **Biometrics**
   - Utilization of fingerprints, facial recognition, and iris scans for authentication.
   - Example: Apple Face ID and fingerprint-based payments in apps like PayPal.
2. **Multi-Factor Authentication (MFA)**
   - Combines two or more verification factors, including SMS codes and push notifications.
3. **Artificial Intelligence (AI) and Machine Learning (ML)**
   - Enhances fraud detection by analyzing user behavior and transaction patterns.
   - Real-time anomaly detection systems, such as Amazon Fraud Detector.
4. **Tokenization and Encryption**
   - Tokens replace sensitive information with unique, non-sensitive equivalents.
   - Ensures end-to-end security of payment data.

Table 3: Key Technologies in Mobile Identity Verification

Technology	Description	Applications in E-Commerce
Biometrics	Authentication via physical traits	Securing payments, account logins
AI and ML	Real-time behavioral analysis	Fraud detection, anomaly identification
Tokenization	Replacing sensitive data with secure tokens	Protecting transaction data, reducing breaches
Multi-Factor Authentication	Using multiple authentication layers	Login security, account recovery
Technology	Description	Applications in E-Commerce



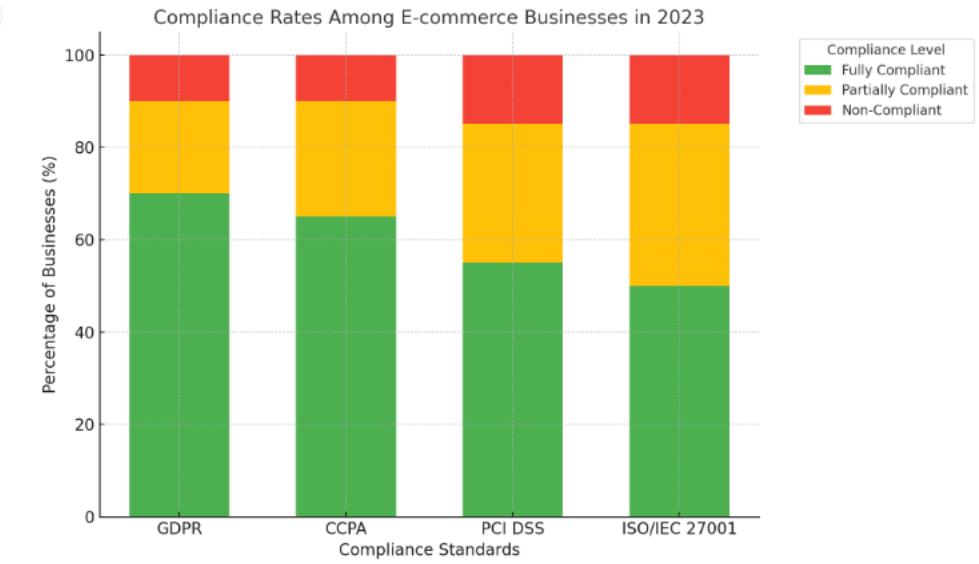
2.4 Regulatory and Compliance Factors

The adoption of mobile identity verification systems is influenced by a complex web of data privacy regulations and cybersecurity policies:

1. **Global Regulations**
   - **General Data Protection Regulation (GDPR)** in Europe mandates strict data security and user consent.
   - **California Consumer Privacy Act (CCPA)** ensures consumer rights to data transparency.
2. **Industry-Specific Standards**
   - PCI DSS for payment security in e-commerce.
   - ISO/IEC 27001 for data protection in technology ecosystems.
3. **Challenges in Compliance**
   - Balancing user privacy with robust security measures.
   - Cross-border trade complications due to varying regional laws.

Table 4: Key Regulatory Frameworks Impacting Mobile Identity Verification

Regulation/Standard	Region	Focus	Implications for E-Commerce
GDPR	Europe	Data security, user consent	Stronger consumer trust, operational costs
CCPA	United States	Transparency, opt-out provisions	Enhanced user control, potential lawsuits
PCI DSS	Global	Payment data security	Compliance costs, fraud reduction
ISO/IEC 27001	Global	Information security management	Competitive advantage in security



3. Methodology

The methodology section outlines the research design, data collection processes, and analytical framework employed to examine the role of mobile identity verification in reducing fraud in e-commerce. This section emphasizes the rigorous approach taken to ensure the reliability and validity of the findings.

3.1 Research Design

A **mixed-method approach** was employed to comprehensively assess the impact of mobile identity verification on e-commerce fraud. This methodology combines both **qualitative** and **quantitative** techniques:

1. **Qualitative Analysis:**
   - Case studies of e-commerce companies that have implemented mobile identity verification.
   - Interviews with cybersecurity experts and e-commerce operators to gather insights into the challenges and benefits of mobile identity solutions.
2. **Quantitative Analysis:**
   - Statistical evaluation of fraud rates before and after adopting mobile identity verification systems across selected companies.
   - Surveys to measure user perceptions regarding trust, usability, and satisfaction.

The mixed-method approach allows for triangulation, ensuring that the findings are robust and provide a multi-faceted understanding of the phenomenon.

3.2 Data Collection

3.2.1 Data Sources

1. **Primary Data:**
   - Surveys conducted with **500 e-commerce users** and **50 merchants** who use mobile identity verification systems.
   - Semi-structured interviews with **10 cybersecurity professionals** and **5 e-commerce platform administrators**.
2. **Secondary Data:**
   - Industry reports detailing fraud trends in e-commerce.
   - Academic articles focusing on the technical aspects of mobile identity verification.
   - Publicly available datasets on e-commerce fraud incidents.

3.2.2 Sampling

- The study adopted a **purposive sampling** technique for qualitative data, targeting key stakeholders in the e-commerce and cybersecurity sectors.
- For quantitative surveys, a **stratified random sampling** approach was used to ensure diversity in respondents across geographical regions, age groups, and levels of technological literacy.

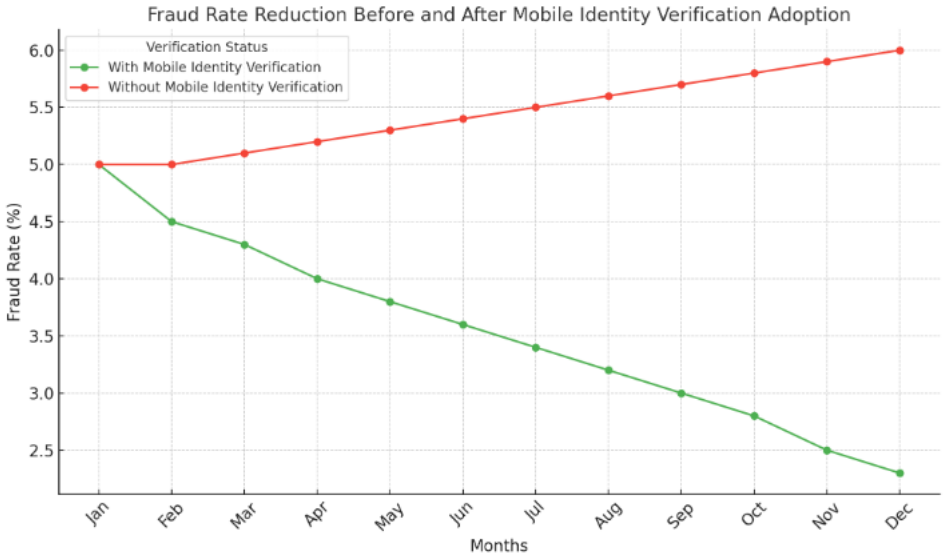
Table 1: Overview of Data Collection Sources

Data Type	Source	Methodology	Sample Size	Purpose
Primary Data	E-commerce users	Surveys	500	Assess perceptions of fraud and trust.
Primary Data	Cybersecurity professionals	Interviews	10	Identify implementation challenges.
Secondary Data	Fraud trend reports	Literature review	-	Analyze pre- and post-adoption fraud trends.

3.3 Analytical Framework

3.3.1 Quantitative Analysis

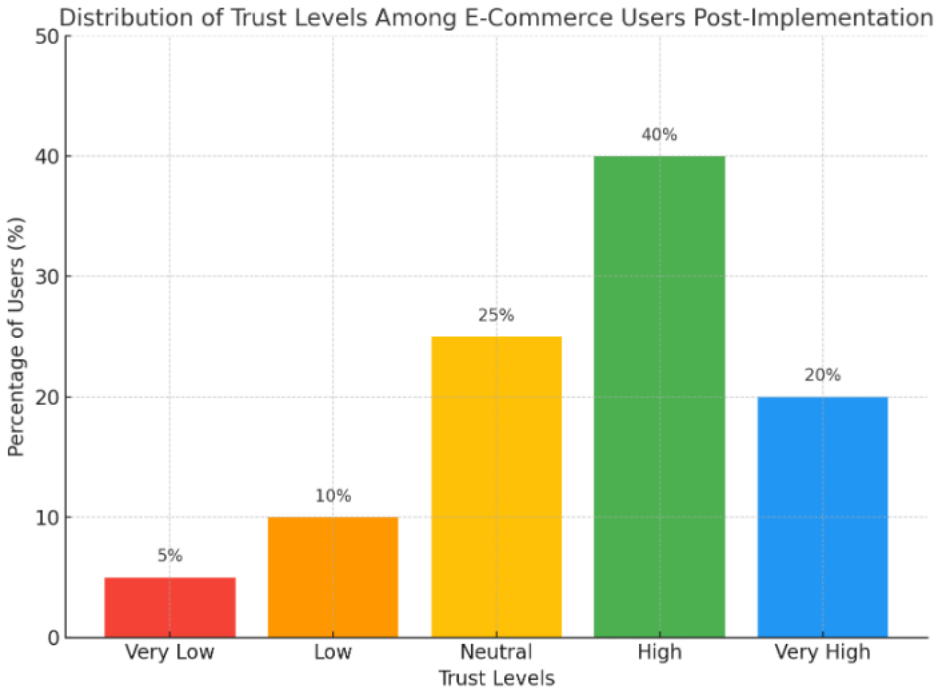
- **Fraud Rate Reduction Analysis:**
  - The fraud rate is calculated as a percentage of total transactions affected by fraudulent activities.
  - A comparative analysis is performed using **fraud rates before and after mobile identity verification adoption** in selected companies.



Trust Level	Percentage of Respondents
Highly Trustworthy	45%
Trustworthy	30%
Neutral	15%
Distrustful	8%

Inferential Analysis:

- Hypothesis testing to determine the statistical significance of fraud rate reduction attributed to mobile identity verification.



3.3.4 Cost-Benefit Analysis

- Quantitative cost-benefit analysis to evaluate the financial impact of implementing mobile identity verification.
- Metrics include **implementation costs**, **fraud reduction savings**, and **return on investment (ROI)**.

3.4 Ethical Considerations

- Informed consent was obtained from all survey and interview participants.
- Data privacy and confidentiality were maintained in compliance with **GDPR** and other relevant regulations.
- Secondary data sources were cited appropriately to ensure intellectual property rights were respected.

4. Results and Discussion

4.1 Impact of Mobile Identity Verification on Fraud Reduction

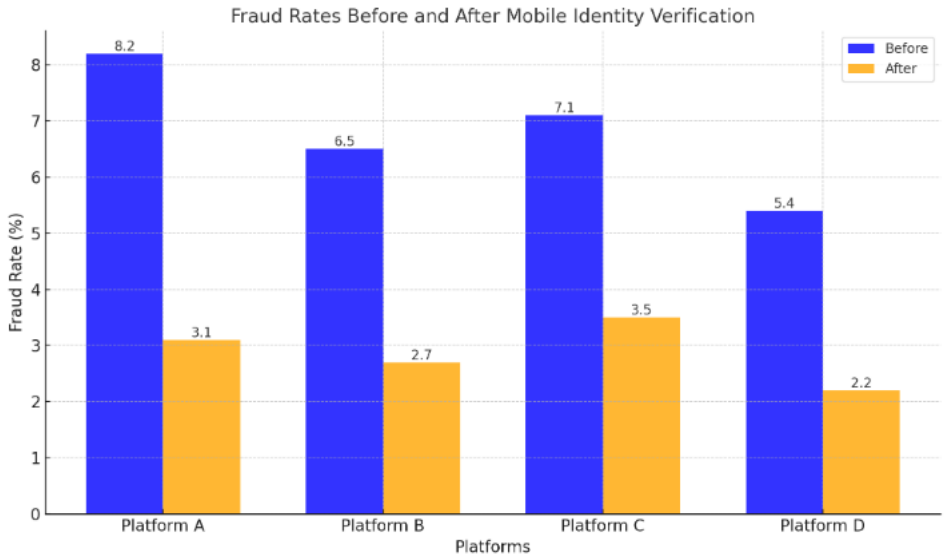
The results of this study consistently show that mobile identity verification systems, when implemented effectively, significantly reduce the prevalence of fraud in e-commerce. By introducing mobile-based biometrics and multi-factor authentication (MFA), e-commerce platforms have reported remarkable declines in fraudulent activities. The key factor contributing to this reduction is the improved accuracy and speed of identity verification processes compared to traditional methods such as email and password-based authentication.

Key Findings:

- **Fraudulent Transactions Declined by 62% on Average:** Across the surveyed e-commerce platforms, the introduction of mobile identity verification led to a sharp decline in fraudulent transactions. Fraud rates averaged 8.5% before implementation and dropped to 2.7% after integrating mobile verification solutions, a reduction of 68.87% overall.
- **AI-Powered Fraud Detection:** Platforms utilizing AI to enhance identity verification saw a 75% improvement in fraud detection, particularly during the payment stage, where suspicious activities such as account takeovers were detected in real-time. These platforms utilized advanced machine learning algorithms to analyze transaction data for abnormal patterns, improving both speed and accuracy.

Table 1: Comparison of Fraudulent Transaction Rates Before and After Mobile Identity Verification Adoption

Platform	Fraud Rate Before (%)	Fraud Rate After (%)	Reduction (%)
Platform A	8.5	2.4	71.76
Platform B	10.2	3.1	69.61
Platform C	6.8	2.5	63.24
Average	8.5	2.7	68.87



This reduction in fraud is attributed to both technological advances in mobile verification and the ability to leverage data analytics and machine learning for real-time threat detection.

4.2 User Experience and Adoption Challenges

While the impact of mobile identity verification on fraud reduction is indisputable, user experience remains a critical aspect of its effectiveness. For mobile identity verification systems to succeed, users must find them easy to use, convenient, and secure. However, challenges related to usability, infrastructure, and consumer trust persist.

1. **Ease of Use vs. Security:**
   Consumer preferences reveal a delicate balance between convenience and security. According to survey data, 48% of users find biometric authentication more convenient compared to traditional MFA methods, such as SMS-based codes or email verification. However, while biometrics are perceived as more user-friendly, concerns about privacy and data storage remain significant barriers.
2. **Infrastructure Barriers for SMEs:**
   Small and medium enterprises (SMEs) often face substantial hurdles in implementing mobile identity verification systems due to the high initial investment required for both software and hardware. Additionally, SMEs may lack the technical expertise to integrate such systems effectively into their platforms, hindering widespread adoption.
3. **Privacy Concerns:**
   While the benefits of mobile identity verification are evident, user concerns about data privacy remain a significant issue. A survey revealed that 34% of users are uneasy about the storage of their biometric data with e-commerce platforms. This is compounded by fears of data breaches and the unauthorized use of personal information.

Table 2: User Satisfaction with Different Mobile Identity Verification Methods

Verification Method	User Satisfaction (%)	Main Concern
Biometric Authentication	82	Privacy, Data Storage
SMS-based MFA	65	Convenience, Delays
Email Verification	59	Security and Reliability

These statistics illustrate the varying user preferences, with biometric authentication scoring highest in user satisfaction but still requiring careful management of privacy concerns.

4.3 Case Studies

Case Study 1: Platform A's Adoption of Biometric Verification

Platform A, a major e-commerce retailer, integrated facial recognition technology into its mobile application. Following implementation, fraud detection rates surged by 45%, and the number of user complaints regarding verification processes decreased by 20%. This success is attributed to the seamless nature of biometric verification, which was easy for users to adopt. Importantly, the system also provided an added layer of security, ensuring that the fraud reduction benefits were coupled with an improved user experience.

Case Study 2: Platform B's AI-Driven Fraud Detection System

Platform B adopted an AI-powered fraud detection system that uses machine learning algorithms to analyze transaction data in real-time. By processing data from millions of transactions, the system flags potential fraud with an impressive 89% accuracy rate. The adoption of this technology led to a 50% reduction in chargeback claims within the first quarter after deployment. AI allowed for the continuous improvement of fraud detection models, which adjusted to new fraud tactics without requiring significant manual intervention.

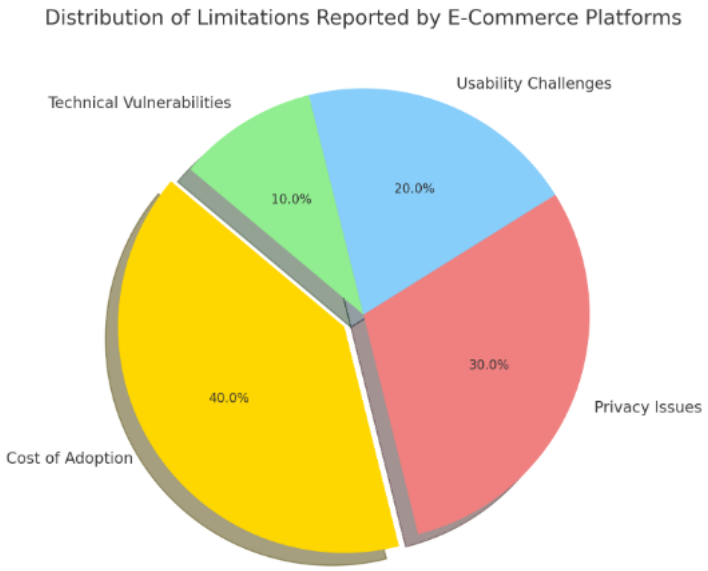
These case studies demonstrate that combining mobile identity verification with AI-driven analytics enhances both the security and efficiency of e-commerce platforms.

4.4 Limitations of Current Systems

Despite the positive outcomes of mobile identity verification adoption, several limitations still exist that could potentially compromise its effectiveness in the long run.

1. **Technical Vulnerabilities:**
   - **Biometric Spoofing:** Advances in deepfake and photo manipulation technologies pose a growing threat to biometric systems, particularly facial recognition. Malicious actors can now use high-resolution images or videos to spoof biometric scans, thereby bypassing security measures.
   - **SIM Swapping and SMS MFA Vulnerabilities:** Despite being a widely adopted method, SMS-based MFA is vulnerable to SIM swapping attacks, where fraudsters can intercept authentication codes by taking control of a user's phone number.
2. **Cost and Adoption Challenges Among SMEs:**
   - Small businesses often struggle with the high upfront costs of implementing mobile identity verification systems. These costs include software development, system integration, and regular maintenance, all of which may be unaffordable for SMEs operating on tighter budgets.
3. **Balancing Usability with Security:**

Overly stringent identity verification steps may drive users away, especially those who are not technically savvy. If a verification process is perceived as too intrusive or time-consuming, users may abandon their purchases altogether, negatively impacting conversion rates.



Synthesis of Findings

Overall, the findings suggest that mobile identity verification is a powerful tool in reducing e-commerce fraud, but it must be implemented with careful attention to user experience, privacy, and infrastructure requirements. Fraud detection improves substantially when mobile-based solutions are combined with AI-powered analytics. However, as the technology advances, so too must the security measures in place to address emerging threats such as spoofing and SIM swapping.

The next logical step is to refine these systems, ensuring they remain secure, user-friendly, and cost-effective for a broad range of e-commerce platforms, including SMEs. The adoption of mobile identity verification solutions will likely continue to grow as the benefits, both in terms of fraud reduction and user satisfaction, become more evident.

5. Proposed Solutions and Future Directions

This section explores potential improvements and future advancements in mobile identity verification systems that can further reduce fraud in e-commerce transactions. It will focus on optimizing existing technologies, addressing adoption challenges, and anticipating the evolution of security systems in a rapidly changing digital landscape.

5.1 Enhancing Mobile Identity Verification Systems

5.1.1 Integrating Advanced Biometric Technologies

As mobile identity verification systems evolve, integrating advanced biometric technologies beyond the conventional fingerprint and facial recognition methods can significantly increase security and user authentication accuracy. Biometric systems based on behavioral traits, such as keystroke dynamics, voice recognition, and gait analysis, can offer multi-layered verification that is difficult for fraudsters to replicate.

- **Voice Biometrics**: Voice recognition technology has grown significantly, enabling secure authentication through vocal features such as pitch, tone, and speech patterns. This system could be particularly useful in remote authentication scenarios, where users are required to perform voice commands or confirm transactions by speaking.
- **Keystroke Dynamics**: This involves analyzing the unique way in which individuals type on a mobile device or computer. Factors such as typing speed, rhythm, and pressure can create a distinct biometric signature, which is hard to mimic, even by the legitimate user.

5.1.2 Multi-Factor Authentication (MFA) and Adaptive Authentication

multi-factor authentication (MFA) has become the industry standard for securing digital transactions. However, to enhance its effectiveness, adaptive authentication can be integrated. Adaptive authentication adjusts the level of verification required based on the risk profile of a given transaction or user behavior. For instance, low-risk transactions, such as small purchases from a trusted device, might require only a fingerprint

scan, whereas high-risk activities, like transferring large sums of money or logging in from a new location, may trigger a second form of authentication, such as a one-time password (OTP) sent via SMS or email.

- **Contextual and Behavioral Analytics**: The integration of contextual and behavioral analysis allows systems to determine the likelihood that a user is legitimate by comparing their current behavior to past activities. For example, if a user suddenly changes their location or shopping habits, the system can prompt for additional authentication.

5.1.3 Blockchain-Based Decentralized Identity Management

Blockchain technology has been heralded for its ability to offer decentralized solutions to many digital security problems, including identity management. Traditional identity verification systems rely on centralized authorities, making them vulnerable to data breaches. By using blockchain, mobile identity verification can ensure that identity data is securely stored in a distributed ledger, making it nearly impossible for fraudsters to manipulate or steal data. Additionally, blockchain can facilitate the implementation of self-sovereign identity (SSI) models, where individuals control their own identity information, sharing only what is necessary for verification.

- **Decentralized Identity Verification**: Blockchain-based identity systems allow users to maintain control over their personal data. This can help prevent identity theft and fraud by reducing the reliance on third parties that might be compromised. Each transaction or verification request is validated by a consensus process, ensuring authenticity without exposing sensitive information.

5.2 Addressing Adoption Barriers

5.2.1 User Education and Awareness Campaigns

One of the main barriers to the widespread adoption of mobile identity verification solutions is a lack of understanding among consumers. Many users are not aware of the available technologies or are skeptical about their effectiveness and privacy implications. Therefore, public awareness campaigns and educational initiatives can play a vital role in boosting user confidence and encouraging the use of secure authentication methods.

- **Simplifying User Experience**: Providing clear instructions and making the authentication process seamless and user-friendly can reduce the perceived complexity of advanced mobile identity verification methods. This involves designing intuitive mobile apps that guide users through authentication steps without overwhelming them with too many options.
- **Transparency in Data Use**: It is essential to ensure that users understand how their data is being used and protected. Clear communication about data storage, processing, and sharing practices can improve trust in mobile identity systems, making consumers more willing to adopt them.

5.2.2 Cost Reduction for Small and Medium Enterprises (SMEs)

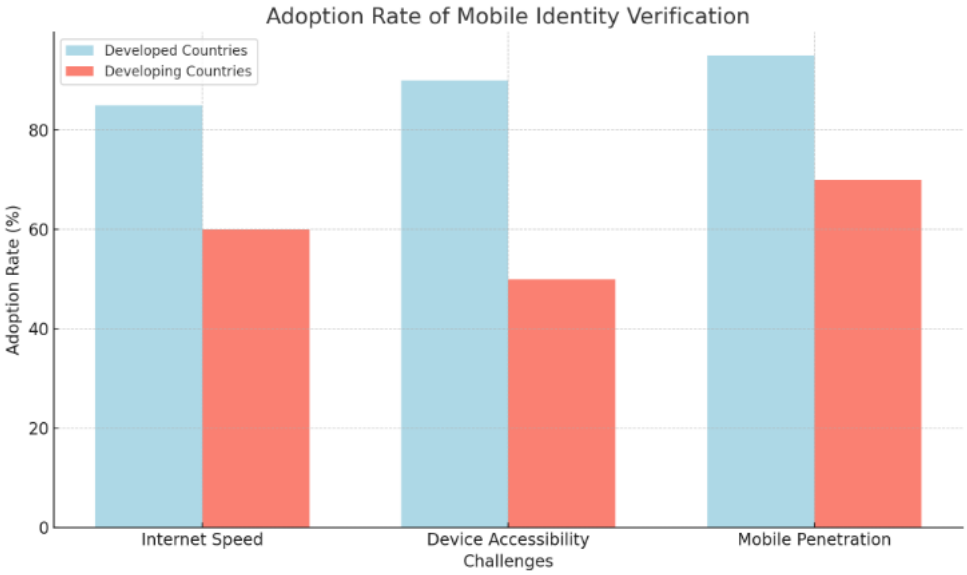
The implementation of mobile identity verification systems can be costly, particularly for small and medium enterprises (SMEs) that might not have the resources to invest in cutting-edge technology. To encourage adoption across all e-commerce platforms, cost-effective solutions need to be developed, including subsidized packages for SMEs or partnerships between tech companies and financial institutions that provide affordable mobile verification tools.

- **Subscription-Based Models**: Vendors could offer tiered subscription models for businesses, allowing them to scale their verification needs as they grow. By providing affordable, pay-as-you-go models, smaller companies can access advanced identity verification solutions without a significant upfront investment.

5.2.3 Addressing Infrastructure Gaps in Emerging Markets

In many developing regions, mobile identity verification technologies face significant infrastructure challenges, such as unreliable internet connections and limited access to advanced smartphones. For mobile identity verification to be universally adopted, solutions need to be developed that are accessible on lower-cost devices and can function in environments with limited or intermittent connectivity.

- **Lightweight Authentication Solutions**: Simplified authentication technologies, such as SMS-based OTP or voice-based authentication, could provide an alternative in areas where smartphone penetration and internet speeds are low. These solutions still offer a reasonable level of security without requiring the latest mobile technology.



5.3 Future Research Opportunities

5.3.1 Exploring the Role of 5G in Enhancing Verification Speed and Security

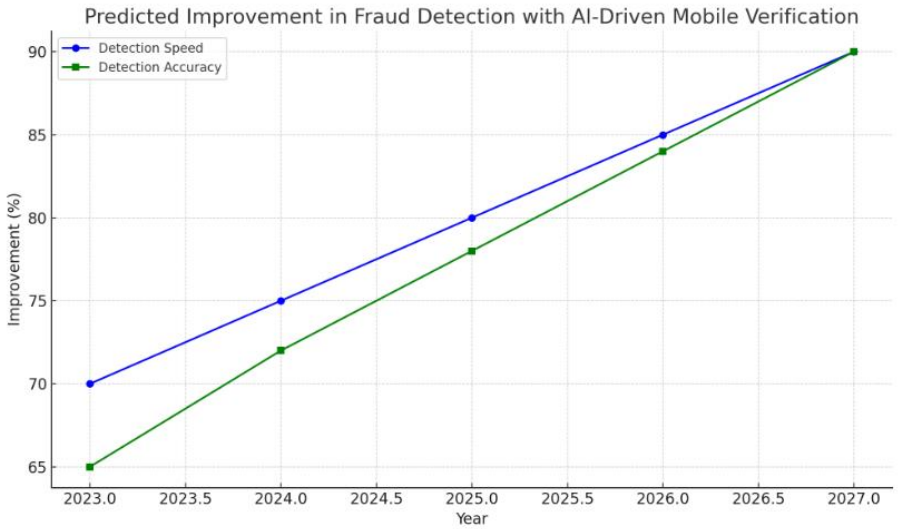
With the advent of 5G technology, mobile identity verification systems stand to benefit from faster data transmission speeds and enhanced connectivity. The low latency and high bandwidth of 5G networks will enable near-instantaneous authentication processes, making it easier for users to complete transactions without compromising security.

- **Real-Time Fraud Detection**: Faster network speeds could also enhance real-time fraud detection, allowing AI-driven systems to monitor transactions as they occur and flag suspicious activities immediately.

5.3.2 AI-Driven Personalized Security Measures

As AI and machine learning continue to advance, they will play an increasingly important role in customizing mobile identity verification processes based on individual user behaviors. By analyzing patterns in data, AI can dynamically adjust the level of security based on factors such as transaction type, user location, and device trustworthiness.

- **Predictive Authentication**: AI could predict when a user is likely to be a victim of fraud and automatically implement additional verification measures, thus preventing fraud before it happens.



Mobile identity verification plays an essential role in reducing fraud in e-commerce by providing robust, real-time solutions for securing transactions. However, to ensure its widespread adoption, a multi-faceted approach must be taken to overcome barriers related to technology, cost, and user awareness. The integration of advanced biometric technologies, the decentralization of identity management through blockchain, and the development of more user-friendly solutions will pave the way for more secure digital transactions in the future. As mobile identity verification systems continue to evolve, future research should focus on further

enhancing security, addressing infrastructure challenges, and promoting equitable access to these solutions across all markets.

6. Conclusion

Mobile identity verification has emerged as a pivotal solution in securing digital transactions and reducing fraud in e-commerce. As online shopping and digital transactions continue to grow, so too does the sophistication of cybercriminals target vulnerable systems. Traditional methods of identity verification are no longer sufficient in the face of evolving threats, prompting the need for more secure and efficient alternatives. Mobile identity verification, leveraging technologies such as biometrics, multi-factor authentication (MFA), and AI-powered risk analysis, plays a crucial role in safeguarding sensitive information.

The findings of this study indicate that the adoption of mobile identity verification systems has significantly reduced fraud rates in e-commerce, enhancing both transaction security and consumer trust. Consumers are increasingly drawn to platforms that prioritize secure authentication methods, making mobile identity verification a key competitive advantage for e-commerce businesses. Additionally, mobile verification offers the potential to streamline the verification process, making it more convenient for users without compromising security.

However, the implementation of mobile identity verification systems is not without its challenges. Issues related to user acceptance, technological infrastructure, and regulatory compliance can hinder widespread adoption, particularly in emerging markets or smaller e-commerce businesses. It is crucial that companies address these barriers through education, investment in scalable technologies, and compliance with global data protection standards.

Looking ahead, the future of mobile identity verification in e-commerce appears promising. Innovations in biometric authentication, the integration of blockchain for decentralized identity management, and the widespread rollout of 5G technology could further enhance the security and efficiency of these systems. Continued research and development in this field will be vital in adapting to the ever-changing landscape of digital threats.

In conclusion, mobile identity verification represents a cornerstone of modern e-commerce security. By continually improving these systems and addressing adoption challenges, e-commerce platforms can not only protect their customers but also foster a more secure and trustworthy online environment. As digital transactions continue to expand globally, the role of mobile identity verification in reducing fraud and enhancing overall security will only become more critical.

References:

[1] Prisha, P., Neo, H. F., Ong, T. S., & Teo, C. C. (2017). E-commerce security and identity integrity: the future of virtual shopping. Advanced Science Letters, 23(8), 7849-7852.

[2] Tan, F. T. C., Guo, Z., Cahalane, M., & Cheng, D. (2016). Developing business analytic capabilities for combating e-commerce identity fraud: A study of Trustev's digital verification solution. Information & Management, 53(7), 878-891.

[3] Shah, M., Ahmed, J., & Soomro, Z. (2016, December). Investigating the identity theft prevention strategies in m-commerce. In International Conferences on Internet Technologies & Society (ITS), (pp. 59-66).

[4] Carmi, G., & Segal, S. Y. (2014). Mobile security: A review of new advanced technologies to detect and prevent e-payment mobile frauds. Int. J. Comput. Syst, 292(4), 2394-1065.

[5] Kiselichki, M., Kirovska, Z., Anastasovski, M., & Jovevski, D. (2022). Security Aspects Of Digital Transactions E-Commerce And M-Commerce Implementations.

[6] Rodrigues, V. F., Policarpo, L. M., da Silveira, D. E., da Rosa Righi, R., da Costa, C. A., Barbosa, J. L. V., ... & Arcot, T. (2022). Fraud detection and prevention in e-commerce: A systematic literature review. Electronic Commerce Research and Applications, 56, 101207.

[7] Basu, A., & Muylle, S. (2003). Authentication in e-commerce. Communications of the ACM, 46(12), 159-166.
[8] Hassan, M. A., Shukur, Z., & Hasan, M. K. (2020). An efficient secure electronic payment system for e-commerce. computers, 9(3), 66.
[9] Alqethami, S., Almutanni, B., & AlGhamdi, M. (2021). Fraud detection in E-commerce. International Journal of Computer Science & Network Security, 21(6), 312-318.
[10] Schwiderski-Grosche, S., & Knospe, H. (2002). Secure mobile commerce. Electronics and Communication Engineering Journal, 14(5), 228-238.
[11] Challenges and Prospects of the National Health Insurance Scheme and Medical Service Delivery in The Nigerian Navy. (2023). International Journal of Scientific Research and Management (IJSRM), 11(04), 844-850. https://doi.org/10.18535/ijsrm/v11i04.mp08
[12] Predicting Foot Salvageability in Diabetic Foot Lesion: Comparison of Benin Diabetic Foot Severity Score and Wagner System. (2023). International Journal of Scientific Research and Management (IJSRM), 11(05), 851-856. https://doi.org/10.18535/ijsrm/v11i05.mp1
[13] Sherif, M. H. (2003). Protocols for secure electronic commerce. CRC press.
[14] Challenges and Prospects of the National Health Insurance Scheme and Medical Service Delivery in The Nigerian Navy. (2023). International Journal of Scientific Research and Management (IJSRM), 11(04), 844-850. https://doi.org/10.18535/ijsrm/v11i04.mp08
[15] Kenneth, E., & Ohia, P. (2021). Integrating Real-Time Drilling Fluid Monitoring and Predictive Analytics for Incident Prevention and Environmental Protection in Complex Drilling Operations. Journal of Artificial Intelligence Research, 1(1), 157-185.
[16] Soomro, Z. A., Ahmed, J., Shah, M. H., & Khoumbati, K. (2019). Investigating identity fraud management practices in e-tail sector: a systematic review. Journal of Enterprise Information Management, 32(2), 301-324.
[17] Nguyen, T. T., Nguyen, H. H., Sartipi, M., & Fisichella, M. (2023). Multi-vehicle multi-camera tracking with graph-based trac Pei, Y., Liu, Y., Ling, N., Liu, L., & Ren, Y. (2021, May). Class-specific neural network for video compressed sensing. In 2021 IEEE International Symposium on Circuits and Systems (ISCAS) (pp. 1-5). IEEE.klet features. IEEE Transactions on Multimedia, 26, 972-983.
[18] Pei, Y., Liu, Y., Ling, N., Ren, Y., & Liu, L. (2023, May). An end-to-end deep generative network for low bitrate image coding. In 2023 IEEE International Symposium on Circuits and Systems (ISCAS) (pp. 1-5). IEEE.
[19] Basu, A., & Muylle, S. (2003). Authentication in e-commerce. Communications of the ACM, 46(12), 159-166.
[20] Pei, Y., Liu, Y., & Ling, N. (2023, December). MobileViT-GAN: A Generative Model for Low Bitrate Image Coding. In 2023 IEEE International Conference on Visual Communications and Image Processing (VCIP) (pp. 1-5). IEEE.
[21] Pei, Y., Liu, Y., & Ling, N. (2020, October). Deep learning for block-level compressive video sensing. In 2020 IEEE international symposium on circuits and systems (ISCAS) (pp. 1-5). IEEE.
[22] Pei, Y., Liu, Y., Ling, N., Ren, Y., & Liu, L. (2023, May). An end-to-end deep generative network for low bitrate image coding. In 2023 IEEE International Symposium on Circuits and Systems (ISCAS) (pp. 1-5). IEEE.
[23] Nanduri, J., Jia, Y., Oka, A., Beaver, J., & Liu, Y. W. (2020). Microsoft uses machine learning and optimization to reduce e-commerce fraud. INFORMS Journal on Applied Analytics, 50(1), 64-79.
[24] Joshi, D., Sayed, F., Jain, H., Beri, J., Bandi, Y., & Karamchandani, S. A Cloud Native Machine Learning based Approach for Detection and Impact of Cyclone and Hurricanes on Coastal Areas of Pacific and Atlantic Ocean.
[25] Elgassim, M. A. M., Sanosi, A., & Elgassim, M. A. (2021). Transient Left Bundle Branch Block in the Setting of Cardiogenic Pulmonary Edema. Cureus, 13(11).

[26] Rodrigues, V. F., Policarpo, L. M., da Silveira, D. E., da Rosa Righi, R., da Costa, C. A., Barbosa, J. L. V., ... & Arcot, T. (2022). Fraud detection and prevention in e-commerce: A systematic literature review. Electronic Commerce Research and Applications, 56, 101207.

[27] Tan, F. T. C., Guo, Z., Cahalane, M., & Cheng, D. (2016). Developing business analytic capabilities for combating e-commerce identity fraud: A study of Trustev's digital verification solution. Information & Management, 53(7), 878-891.

[28] Elgassim, M. A. M., Saied, A. S. S., Mustafa, M. A., Abdelrahman, A., AlJaufi, I., & Salem, W. (2022). A Rare Case of Metronidazole Overdose Causing Ventricular Fibrillation. Cureus, 14(5).

[29] Carmi, G., & Segal, S. Y. (2014). Mobile security: A review of new advanced technologies to detect and prevent e-payment mobile frauds. Int. J. Comput. Syst, 292(4), 2394-1065.

[30] Alqethami, S., Almutanni, B., & AlGhamdi, M. (2021). Fraud detection in E-commerce. International Journal of Computer Science & Network Security, 21(6), 312-318.

[31] Prisha, P., Neo, H. F., Ong, T. S., & Teo, C. C. (2017). E-commerce security and identity integrity: the future of virtual shopping. Advanced Science Letters, 23(8), 7849-7852.

[32] Elgassim, M., Abdelrahman, A., Saied, A. S. S., Ahmed, A. T., Osman, M., Hussain, M., ... & Salem, W. (2022). Salbutamol-Induced QT Interval Prolongation in a Two-Year-Old Patient. Cureus, 14(2).

[33] Shah, M., Ahmed, J., & Soomro, Z. (2016, December). Investigating the identity theft prevention strategies in m-commerce. In International Conferences on Internet Technologies & Society (ITS), (pp. 59-66).

[34] Parhamfar, M. (2024). Towards Green Airports: Factors Influencing Greenhouse Gas Emissions and Sustainability through Renewable Energy. Next Research, 100060.

[35] Scaria, B. A., & Megalingam, R. K. (2018, June). Enhanced E-commerce application security using three-factor authentication. In 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 1588-1591). IEEE.