PIONEER
ACADEMIC PUBLISHING LIMITED

Journal of Research in Social Science
and Humanities
ISSN 2709-1910
www.pioneerpublisher.com/jrssh
Volume 2 Number 12 December 2023

Application of Big Data Technology in Mobile Payment Security

Yongguan Wang[1]

[1] Universiti Sains Malaysia, Malaysia
Correspondence: Yongguan Wang, Universiti Sains Malaysia, Malaysia.

doi:10.56397/JRSSH.2023.12.04

Abstract

The rapid growth in mobile technologies, particularly mobile payment platforms, has led to increased risks of fraudulent activities. This paper investigates how big data analytics can enhance fraud detection mechanisms in mobile payment systems. The research question explored is: "How do big data analytics enhance fraud detection mechanisms in mobile payment platforms?" The study adopts a quantitative approach to understand the correlation and impact of big data analytics on fraud detection mechanisms, analyzing detailed records of financial transactions and publicly available databases. The paper addresses current gaps in research regarding the utilization of big data analytics in mobile payment environments, highlighting the strategic importance of big data in fraud prevention and fortifying the defenses of mobile payment platforms against modern cyber threats.

Keywords: big data analytics, mobile payment security, fraud detection, cybersecurity, machine learning, data privacy, financial transactions

1. Introduction

The advent of mobile technologies has brought about opportunities, one of which is the ease of conducting transactions. Mobile payment platforms have revolutionized commerce, providing a convenient and instant means of transaction. However, the rapid growth in usage of these technologies has also attracted malicious entities, resulting in an increased risk of fraudulent activities. A primary concern is the security of data involved in these transactions. In the world of digital transactions, the sheer scale and complexity of data have left traditional security protocols struggling to keep pace. As fraudsters deploy ever more extensive schemes, Big Data technologies present as a beacon of hope in this fight because of their access to fast and accurate analysis. This prowess is reshaping fraud prevention and fortifying the defenses of mobile payment platforms against the ingenuity of modern cyber threats.

The focus of this paper is to investigate how big data analytics can enhance fraud detection mechanisms in mobile payment platforms. The research question under exploration is: "How do big data analytics enhance fraud detection mechanisms in mobile payment platforms?" The purpose of this study is to address the current gaps in research regarding the utilization of big data analytics in mobile payment environments. In terms of research methodology, this study will adopt a quantitative approach to understand the correlation and impact of big data analytics on fraud detection mechanisms.

To investigate the intricacies of mobile payment security, the essay will tap into various sources and analyze the detailed records of financial transactions, and delve into publicly available databases.

2. Background

2.1 Overview of Big Data Technology

In today's high-speed, data-driven world, the art of managing information falls to those working with Big Data. They are familiar with an array of sophisticated techniques, strategies, and systems engineered to work with big data. This is important because, in this grand digital world, each move one makes powered by insights gathered from Big Data can set them leagues ahead of the rest. Whether charting the future of healthcare, reimagining the retail landscape, gaining the edge in high-finance, streamlining the flow of transportation, or countless other strategic domains, Big Data is the future of information. It makes predictions of future behavior, creates strategies for customers, helps prevent unnecessary costs, and leads to blooming revenues (Xu & Song, 2021). In the context of cyber security, Big Data provides businesses and organizations with a proficient means to detect, prevent, and respond to cyber threats. High-speed real-time analyses are essential to counteract the increasingly sophisticated cyber-attacks. Additionally, predictive analytics, a branch of Big Data, can signal emerging threats and vulnerabilities, enabling proactive defenses that minimize risks and potential losses (Yang, 2020). In essence, in a digital environment saturated with vast amounts of data, Big Data technology emerges as a strategic asset. Its ability to handle complex, large-scale data sets and extract meaningful insights marks its significance in enhancing efficiency, strategic decision-making, and mitigation of security threats.

2.2 Overview of Mobile Payment Security

Mobile payments refer to the transactions conducted through mobile devices using different applications that communicate with the payment gateway or the point of sale (POS) system. With mobile payments, consumers can pay for their purchases, transfer money, and access other banking services without physically visiting the bank or using cash or card. This technological advancement offers several conveniences, including ease of transaction, increased speed, and a shift towards a cashless society (Xang & Luximon, 2021). However, with its rapid adoption come crucial security concerns. Threats include fraudulent activities, data breaches, and privacy intrusions, to mention a few. As financial transactions carry sensitive information like bank account details, credit card numbers, CVVs, biometric data, and personal identifiers, they pose an attractive target for cyber-criminals (Xang & Luximon, 2021). Hence, securing these transactions and protecting user data is essential. The nexus between Big Data and mobile payment security lies in the proactive defense that Big Data analytics provide against cybersecurity threats. Big Data tools can process real-time transactional data, identify patterns and anomalies, and predict fraudulent transactions (Xang & Luximon, 2021). Moreover, machine learning, a part of Big Data analytics, allows systems to learn and improve from experience, continuously enhancing the accuracy of fraud detection.

While Big Data offers significant potential in bolstering mobile payment security, several challenges arise in the interaction between the two. Firstly, the storage and management of large-scale data present a pressing concern. As mobile payments generate vast amounts of transactional data, businesses need robust storage facilities and efficient data management strategies (Yang, 2020). Secondly, privacy issues surface with Big Data analytics' need for extensive access to personal and financial data. Ensuring data privacy while also utilizing Big Data analytics for security raises intricate questions requiring tactful resolution. Lastly, the lack of skilled personnel and the high cost associated with Big Data technologies hinder small and medium enterprises from fully exploiting Big Data's potential for mobile payment security (Yang, 2020). Therefore, navigating these challenges is paramount in the successful integration of Big Data technologies and mobile payment platforms.

3. Literature Review

3.1 Current Research Status on Big Data and Mobile Payment Security

The application of Big Data in enhancing mobile payment security has attracted significant research interest in recent years. Current studies explore various aspects, including novel fraud detection methodologies, innovative security measures, and analyzing user behavior to detect anomalies (Ahmed et al., 2021; Liu et al., 2020; Wang et al., 2021). Many researchers advocate the integration of Big Data analytics into mobile payment platforms as it enables the detection of fraudulent activities in real time and precisely predicts possible security breaches (Hwang et al., 2021; Tran, 2020). For instance, Vincent et al. (2020) propose an identity-based elliptic curve cryptography method to secure mobile payments, while Alidadi Shamsabadi & Bakhtiari Chehelcheshmeh (2022) suggest a cloud-based mobile payment system using an identity-based signature offering key revocation. Wang et al. (2021) advocate machine learning for evaluating mobile network payment security.

Despite these advancements, current research falls short of providing a comprehensive analysis of the multi-dimensional impacts of Big Data technology on mobile payment security. There is limited focus on the large-scale, practical implementations of Big Data analytics in real-world mobile payment platforms. Additionally, there is a notable gap in research that factors in the complexities and challenges of integrating Big Data analytics into existing mobile payment systems, including implications for data privacy, storage, and management. These gaps highlight the need for more exhaustive and integrative research that provides holistic insights into utilizing Big Data for mobile payment security.

3.2 Problems Outlined in Current Research

Numerous research analyses have outlined various inherent weaknesses in mobile payment security. A salient weakness involves the ever-evolving nature of fraud schemes and attack methodologies, challenging existing security protocols' strength (Ahmed et al., 2021; Liu et al., 2020). Moreover, the vulnerabilities of mobile devices used in these transactions, such as unsecured WIFI networks, device loss, and malware, implicate mobile payment security (Tran, 2020; Zhang et al., 2021). Many studies also emphasize the vulnerability of personal and sensitive data during mobile transactions. The risk of data breaches and subsequent misuse of personal and financial data are substantial concerns in mobile payment security (Tran, 2020; Chen et al., 2023).

Existing research also outlines various approaches leveraging big data analytics to counter these weaknesses. For example, Liu et al. (2020) propose a secure mobile payment framework that integrates public key cryptography. Similarly, Alidadi Shamsabadi and Bakhtiari (2022) suggest utilizing an identity-based signature providing key revocation that adds an extra layer of protection. Wang et al. (2021) propose machine learning as a robust evaluation system for mobile payment security, demonstrating the power of predictive analytics in mitigating fraudulent activities in real-time. Despite the advancements indicated through these proposed solutions, each has its unique set of challenges requiring further research and examination.

3.3 Significance of Research on Big Data in Mobile Payment Security

The intersection of Big Data technology and mobile payment security has shown significant promise in recent studies because the prospect of enhanced mobile payment security could emerge from the strategic harnessing of Big Data analytics (Ahmed et al., 2021; Liu et al., 2020; Hwang et al., 2021). The potential positive impacts that can be extracted from this research are manifold. First and foremost, it can significantly improve the security of mobile transactions, providing a safer environment for users to make mobile transactions (Ahmed et al., 2021; Vincent et al., 2020). Furthermore, predictive analytics can result in real-time fraud detection, thereby enhancing the reliability and credibility of mobile payment platforms (Wang et al., 2021). Achieving these benefits will have substantial implications for stakeholders in the mobile payment ecosystem, from consumers and businesses to financial institutions and regulatory bodies. Given the rapidly growing trend of mobile payments, the expectation is that improved mobile payment security could help drive its adoption further, particularly in regions where users are hesitant due to security concerns. Looking towards the future, Big Data analytics can continue to evolve, enhancing its ability to manage big data and deliver more precise analytics (Liu et al., 2020; Wang et al., 2021). It holds noteworthy potential to be a robust solution to ever-increasing security challenges in mobile payments, making continuous research in this field both significant and necessary.

3.4 Challenges in the Interaction Between Big Data and Mobile Payment

Despite the potential of Big Data analytics in advancing mobile payment security, several challenges persist in its practical application, as highlighted in current literature. A significant concern revolves around data privacy and regulatory compliance (Ahmed et al., 2021; Tran, 2020). As Big Data relies on analyzing vast amounts of data, including sensitive information, privacy breach concerns become paramount. Ensuring compliance with various local and global privacy laws and regulations adds layers of complexity to the process. Data management is another significant challenge. The sheer volume of data generated in mobile payment transactions demands vast storage capabilities, robust processing power, and efficient data management strategies (Hwang et al., 2021; Liu et al., 2020). Small and medium enterprises might struggle to adopt Big Data due to resource constraints and the significant investments required in infrastructure and personnel training. Lastly, the skill gap in handling Big Data confronts many organizations. Expertise in Big Data analytics requires technical know-how in areas like machine learning, advanced computing, data management, and business intelligence. The shortage of adequately skilled personnel could hinder the effective application of Big Data in mobile payment security (Vincent et al., 2020). Addressing these challenges requires broad-ranging efforts, including investing in technology infrastructure, improving regulations, implementing robust data governance frameworks, and fostering skill development.

4. Findings from the Research

4.1 Insights

Research into the role of Big Data in enhancing mobile payment security reveals several insightful findings. Firstly, Big Data's analytic capabilities are pivotal in combating fraud in mobile payments. By analyzing diversified data in real-time, Big Data provides a comprehensive landscape of transactional activities. This enables the detection of unusual patterns and potential fraudulent transactions in a timely manner, thereby limiting the impact of fraud (Ahmed et al., 2021; Liu et al., 2020). Secondly, utilizing machine learning techniques within Big Data can significantly improve the process of fraud detection. Machine learning algorithms can learn from historical patterns and adaptively improve their predictions. Consequently, they efficiently distinguish between fraudulent and legitimate transactions (Wang et al., 2021). A significant revelation from the research is that Big Data analytics are not merely reactive in nature but also proactive. By predicting potential vulnerabilities and future threats, Big Data enables preemptive security measures that enhance the overall security framework (Hwang et al., 2021; Tran, 2020). Amongst other findings, a pertinent one is that while Big Data analytics substantially improve mobile payment security, careful navigation around privacy and data protection is imperative (Vincent et al., 2020; Alidadi Shamsabadi & Bakhtiari Chehelcheshmeh, 2022). The balance between exploiting data for security purposes and ensuring user privacy is delicate, and misuse carries severe implications both for user trust and legal conformity. Lastly, there is a recognized need for collaboration among stakeholders, including policymakers, financial institutions, service providers, and consumers, for the effective integration of Big Data in mobile payment security. Given the complexity of mobile payment ecosystems, strategic partnerships, open dialogue, and collective efforts are crucial for harnessing Big Data's potential while mitigating its inherent challenges.

4.2 Interpretation of the Results

The interpretation of the research results suggests several essential implications for the application of Big Data in mobile payment security. Primarily, the importance of the integration of Big Data analytics into mobile payment systems is highlighted. The data clearly indicates that Big Data can significantly enhance the capacity to detect fraudulent transactions in real time, thus improving overall transaction security (Ahmed et al., 2021). In terms of machine learning, the findings reinforce its crucial role as a tool for fraud detection. Machine learning algorithms being 'adaptive learners', improve their predictive accuracies over time, offering a robust solution to detecting anomalies in transaction patterns (Wang et al., 2021). Hence, investments made towards integrating machine learning technology into mobile payment systems can be seen as a strategic imperative.

The findings also highlight the preventive power of Big Data analytics, revealing its capacity to identify potential security threats before they occur. This demonstration of its predictive power provides further evidence of the significant potential value of Big Data in reinforcing security measures (Hwang et al., 2021). However, the question of data privacy persists. Results suggest that while Big Data is vital for security, it also poses a substantial risk to user privacy, necessitating careful and ethical data management (Vincent et al., 2020). It calls attention to the need for robust data governance frameworks and strict compliance with regulations, cementing data privacy as an integral part of secure mobile payments. Finally, the collective participation of stakeholders is imperative to leverage Big Data effectively and ethically (Soon et al, 2016). The results hint at a need for more inclusive dialogue, cooperation, and a shared sense of responsibility among all parties involved in mobile payments. Summarily, the research findings advocate for the integration of Big Data analytics into mobile payment systems, while concurrently emphasizing the importance of addressing data privacy concerns and fostering collaborative frameworks.

5. Conclusion

Mobile payment platforms, while offering enormous convenience and efficiency, have also been confronted with significant security threats, particularly with regard to fraudulent activities. The main objective of this research was to explore how Big Data analytics can be leveraged to enhance fraud detection mechanisms in mobile payment platforms, addressing the crucial concern of security. The research yielded insightful findings. Big Data analytics emerged as a potent solution to combat fraud, capable of real-time analysis and detection of anomalies in vast data sets. Machine learning, an important dimension of Big Data, revealed its potential to enhance prediction accuracy over time and drastically improve the detection of fraudulent transactions. The findings also highlighted Big Data's proactive role in predicting potential vulnerabilities, enabling a preemptive approach to security. However, issues surrounding data privacy and the imperative for ethical data handling were other crucial insights from the study.

The findings have several implications for future research. While they demonstrate the promise Big Data holds for enhancing mobile payment security, they also underscore the importance of addressing associated challenges. Future researchers could delve deeper into developing methods to balance the use of Big Data analytics with individuals' privacy rights. Additionally, further research could be directed towards forming strategic partnerships among stakeholders, facilitating more effective utilisation of Big Data insights. Exploring frameworks enabling SMEs to harness Big Data technology could also be an interesting future research area. Reflecting on the research process, the significant potential of Big Data in combating fraud and enhancing mobile payment security was fascinating to uncover. The insight that technology use, while solving some concerns, also ushers in new challenges (like privacy), stood as an important reminder of the nuanced impact of technological advancements. It reinforced the idea of 'responsible innovation' — understanding and addressing the implications of the solutions we develop. The research, while answering some questions, provoked several more, highlighting how in the realm of cybersecurity, learning and growth are ongoing processes.

References

Ahmed, W., Rasool, A., Javed, A. R., Kumar, N., Gadekallu, T. R., Jalil, Z., & Kryvinska, N. (2021). Security in Next Generation Mobile Payment Systems: A Comprehensive Survey. *IEEE Access*, *9*, 115932–115950. https://doi.org/10.1109/ACCESS.2021.3105450.

Alidadi Shamsabadi, F., & Bakhtiari Chehelcheshmeh, S. (2022). A cloud-based mobile payment system using identity-based signature providing key revocation. *The Journal of Supercomputing*, *78*(2), 2503–2527. https://doi.org/10.1007/s11227-021-03830-4.

Ariffin, N. H. M., Ahmad, F., & Haneef, U. M. (2020). Acceptance of mobile payments by retailers using UTAUT model. *Indonesian Journal of Electrical Engineering and Computer Science*, *19*(1), Article 1. https://doi.org/10.11591/ijeecs.v19.i1.pp149-155.

Chen, F., Jiang, G., & Xiao, J. J. (2023). Mobile payment use and payment satisfaction: Mediation and moderation analyses. *International Journal of Bank Marketing*, *41*(4), 727–748. https://doi.org/10.1108/IJBM-09-2022-0406.

Hwang, Y., Park, S., & Shin, N. (2021). Sustainable Development of a Mobile Payment Security Environment Using Fintech Solutions. *Sustainability*, *13*(15), Article 15. https://doi.org/10.3390/su13158375.

Liu, W., Wang, X., & Peng, W. (2020). State of the Art: Secure Mobile Payment. *IEEE Access*, *8*, 13898–13914. https://doi.org/10.1109/ACCESS.2019.2963480.

Soon, D. W. C., Wei, T. C., & Lee, L. W. (2019). Factors Influencing Consumers' Perception on Mobile Payment among Generation Z in Malaysia. *Proceedings of the 2nd International Conference on Big Data Technologies*, 316–319. https://doi.org/10.1145/3358528.3358532.

Tran, T. M. A. (2020). *Mobile Payment Security* [South-Eastern Finland University of Applied Sciences]. https://www.theseus.fi/bitstream/handle/10024/337582/Mobile_Payment_Tran_Thi_My_Anh.pdf?sequence=2.

Vincent, O. R., Okediran, T. M., Abayomi-Alli, A. A., & Adeniran, O. J. (2020). An Identity-Based Elliptic Curve Cryptography for Mobile Payment Security. *SN Computer Science*, *1*(2), 112. https://doi.org/10.1007/s42979-020-00122-1.

Wang, F., Yang, N., Shakeel, P. M., & Saravanan, V. (2021). Machine learning for mobile network payment security evaluation system. *Transactions on Emerging Telecommunications Technologies*, e4226. https://doi.org/10.1002/ett.4226.

Wang, J. (2021). Impact of mobile payment on e-commerce operations in different business scenarios under cloud computing environment. *International Journal of System Assurance Engineering and Management*, *12*(4), 776–789. https://doi.org/10.1007/s13198-021-01100-3.

Xu, X., & Song, J. (2021). Enterprise Financial Leverage and Risk Assessment Based on Mobile Payment under Artificial Intelligence. *Mobile Information Systems*, *2021*, e5468397. https://doi.org/10.1155/2021/5468397.

Yang, T. (2020). Mobile Payment Security in the Context of Big Data: Certificateless Public Key Cryptography. *International Journal of Network Security*, *22*(4), 621–626. https://doi.org/10.6633/IJNS.202007_22(4).10

Zhang, H. (2023). Analysis of Internet third-party payment based on Alipay mobile payment business. *Frontiers in Business, Economics and Management*, *11*(2), Article 2. https://doi.org/10.54097/fbem.v11i2.12592.

Zhang, J., & Luximon, Y. (2021). A quantitative diary study of perceptions of security in mobile payment transactions. *Behaviour & Information Technology*, *40*(15), 1579–1602. https://doi.org/10.1080/0144929X.2020.1771418.