Proceedings of the 3rd International Conference on Management Research and Economic Development
DOI: 10.54254/2754-1169/171/2025.21861

The Integration of IoT into Fintech: Enhancing Payment Systems and Security – A Case of PayPal

Linlan Zou[1,a,*]

[1]*The University of New South Wales, Sydney, 2025, Australia*
a. linlanzou@gmail.com
**corresponding author*

Abstract: This study took PayPal as a case to explore the Integration of the Internet of Things (IoT) into financial technology (fintech) and focused on the impacts of IoT on payment systems and security enhancements. This study carried out an online questionnaire survey on 65 valid respondents who were PayPal users in Australia. Through the quantitative analysis of the collected survey data, the study argues that the IoT can greatly enhance PayPal's payment ecosystem by improving user convenience, automated payments, and seamless and contactless transactions. Additionally, biometric authentication that is enabled by IoT can significantly reduce unauthorised access; and PayPal's advanced real-time fraud detection system can largely reduce fraudulent transactions and enhance financial security. Whereas, this study also finds the challenges of integrating IoT into fintech, mainly including data privacy issues and concerns about unauthorised access. Through the PayPal case study, this study demonstrates the practical applications of IoT in fintech, and highlights the potential and challenges of such integration. This study recommends that future research may involve as many comparative cases of financial institutions as possible, investigate larger samples, and investigate the intersection of IoT with emerging technologies (such as AI, edge computing, etc.) in the context of fintech. It is hoped that these insights will provide effective guidance for financial institutions, technology providers, and policymakers.

Keywords: Internet of Things (IoT), financial technology (fintech), payment systems, security enhancement, PayPal

1. Introduction

In recent years, with the development of technology, the digital field represented by the Internet of Things (IoT) has begun to rapidly integrate into financial technology (fintech) to increase payment security. Established in California in December 1998, PayPal is both a valuable fintech firm and a leading digital payment firm in the world. It has a huge company size and high brand influence worldwide [1]. Thus, PayPal is a classic case for this study to explore the impacts of IoT integration into fintech. In particular, the payment systems and security areas have created innovative solutions to reshape the financial sector. The integration of IoT into fintech has facilitated real-time data collection and analysis, the development of smarter financial decisions, and the launch of personalised financial products [2]. The integration of the two has a wide range of applications, such as smart payment systems, IoT-driven supply chain finance, etc. [3]. However, fewer researchers have studied the integration of IoT into fintech to enhance payment systems and security, which is the major gap

DOI: 10.54254/2754-1169/171/2025.21861

in research. Through the analysis of PayPal's IoT integration, this study aims to gain some unique insights into the impacts of IoT integration into fintech on the enhancement of payment systems and security.

This study will first critically review the literature on IoT in fintech, IoT in payment systems, IoT and financial security, and challenges of integrating IoT into fintech. Then, it will justify the methodology. Next, it will analyse and discuss the research findings, using PayPal as a case to illustrate the integration of IoT into fintech. Finally, it will summarise the main findings and make recommendations for future research.

2. Literature Review

2.1. IoT in fintech

Dange [4] defined IoT as an interconnected network of physical devices that enable data collection and exchange, embedded electronics, software, sensors, and network connectivity. In terms of fintech, IoT involves a range of devices and technologies that facilitate financial transactions and services, with key components of smart devices, sensors and connectivity technologies, data analytics, and cloud computing infrastructure [3]. According to some researchers [3, 5], IoT has realised rapid growth and widespread applications in the fintech field due to the growing demand for digital transformation, personalised financial services, and enhanced security measures. By integrating into fintech, IoT helps financial institutions to understand customer behaviours and preferences in real-time and provide them with highly personalised service experiences [5].

2.2. IoT in payment systems

While IoT has brought transformative changes to fintech broadly, its impact is most noticeable in payment systems, where seamless and contactless transactions have redefined user experiences. According to the research of some scholars [6, 7], the integration of IoT and payment systems has made great progress in three major aspects. In seamless and contactless transactions, AL-Tamimi et al. [6] believed that IoT devices represented by smartphones and wearable devices have become an important part of modern payment ecosystems. Gkonis et al. [7] considered automated payment processes through IoT integration as another significant advance in payment systems, because it highlights how IoT devices can autonomously initiate and complete transactions based on predefined conditions or user preferences. The combination of the two also gave birth to the concept of invisible payments, where transactions take place in the background without explicit actions by users [8]. Third, in terms of user convenience enhancement, the integration of IoT with payment systems streamlines payment processes in a variety of environments, shortens transaction times, and improves user experiences through personalisation and situational awareness[9].

2.3. IoT and financial security

In academic, some scholars [2, 10-13] have found that the integration of IoT with financial systems introduces a new paradigm for security measures in biometric authentication, real-time fraud detection, secure data transmission and storage, and other areas.

Some scholars [10, 11] considered that biometric authentication has become a powerful tool to enhance financial security. For example, IoT devices can leverage a variety of biometric patterns (such as fingerprints, facial recognition, voice recognition, etc.) to enhance the security of financial services, which underscores their potential to greatly reduce identity theft and unauthorised access [10]. However, Fernandez-Caramés et al. [11] argued that biometric authentication helps improve security, but it could also raise privacy concerns and cause differences in user demographics and

DOI: 10.54254/2754-1169/171/2025.21861

environmental conditions. It is essential to ensure the reliability and accuracy of biometric data collection.

IoT protects financial security through real-time data analysis, thus changing the ability of real-time fraud detection. According to Fazel et al. [12], IoT sensors and devices can continuously monitor transaction patterns and user behaviours, and quickly determine possible fraudulent activities. Additionally, secure data transmission and storage are also important in the IoT financial system. Lu [13] believed that the IoT's combination with blockchain technology can effectively guarantee transparent and safe financial transactions. In the opinion of Bagria et al. [3], blockchain technology provides immutable records of financial data that the IoT generates, which contributes to generating decentralised and tamper-proof ledgers and improves the traceability and integrity of data.

2.4. Challenges of integrating IoT into fintech

Despite the above advancements, the integration of IoT into fintech also poses significant challenges, particularly in terms of data privacy, standardisation, and regulatory compliance.

Data privacy was widely regarded by scholars as a major challenge to integrate IoT into fintech. According to Kshetri [2], the widespread adoption of IoT devices in the financial ecosystem may lead to the collection of sensitive financial data and increase the risk of unauthorised access and potential abuse. Hussein [10] believed that the operability and scalability issues are also a major challenge to integrate IoT into fintech. The differences in standardised protocols and interface standards in different countries greatly affect the seamless integrations of diverse IoT devices and systems, which may restrict the potential of IoT in fintech [14]. Moreover, applying existing regulatory compliance and standards to IoT services is also a big challenge. Through relevant research, Dafri et al. [15] found that the speed of technological innovation usually exceeds the regulatory framework, which creates a certain gap in market stability and consumer protection.

3. Methodology

To solve the research question of how PayPal's integration of IoT into fintech can enhance payment systems and security, the positivist research paradigm was used in this study. This paradigm assumes that reality is objective and measured by scientific methods [16]. Under this paradigm, this study adopted the quantitative research method of questionnaire survey to study the research question. In order to collect the primary data of PayPal users, this study compiled a structured, closed-ended questionnaire covering 15 questions. The questionnaire consisted of four parts, focusing on PayPal users' perceptions and views on using the IoT-enabled payment system, security functions, and challenges. These questions mainly adopted the 5-point Likert scale design. This conformed to the positivist research paradigm, and the researcher could collect quantifiable data and statistically analyse it [17]. Due to the strong convenience and low investigation cost [18], the convenient sampling method was adopted in this study. The target group included active users of PayPal in Australia who have used the IoT payment functions in the past three months. The researcher used social media to get the participants. Moreover, this study collected data through an online questionnaire that was posted on a popular online survey platform SurveyMonkey (https://www.surveymonkey.com/). Compared to the offline survey, the online questionnaire survey was more convenient, had lower costs, and enabled the researcher to approach participants in a wider range of regions [19]. The researcher pre-tested the questionnaire in a small pilot group to guarantee that the questions were clear and reliable [16].

DOI: 10.54254/2754-1169/171/2025.21861

4. Findings and Discussion

In this study, the researcher invited 100 PayPal users in Australia to take part in the online questionnaire survey; and 65 users completed the questionnaire. Based on the data of these valid respondents, this study made a quantitative analysis of it and obtained the following findings.

4.1. Demographic information of respondents

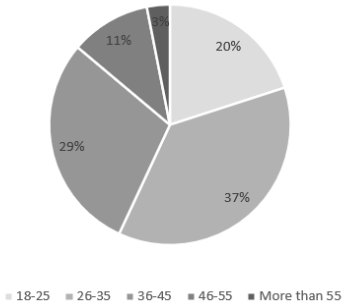

Figure 1: Respondents' age groups

Among 65 respondents, there were 24 users aged 26-35, followed by 19 users aged 36-45 and 13 users aged 18-25. These three groups accounted for the total proportion of 86%. In comparison, there were fewer users aged more than 45 (see Figure 1).

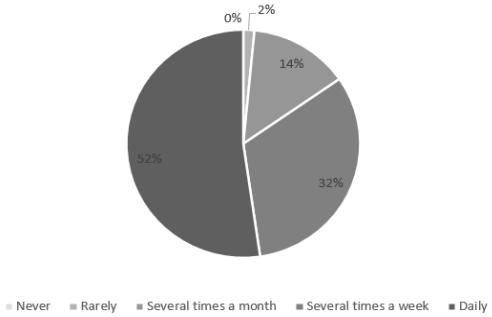

Figure 2: Frequency of respondents' use of PayPal

As presented in Figure 2, all respondents used PayPal. 34 respondents (52%) used PayPal daily, followed by several times a week (21, 32%). Both groups took the proportion of 84%. Relatively, fewer respondents used PayPal several times a month or rarely.

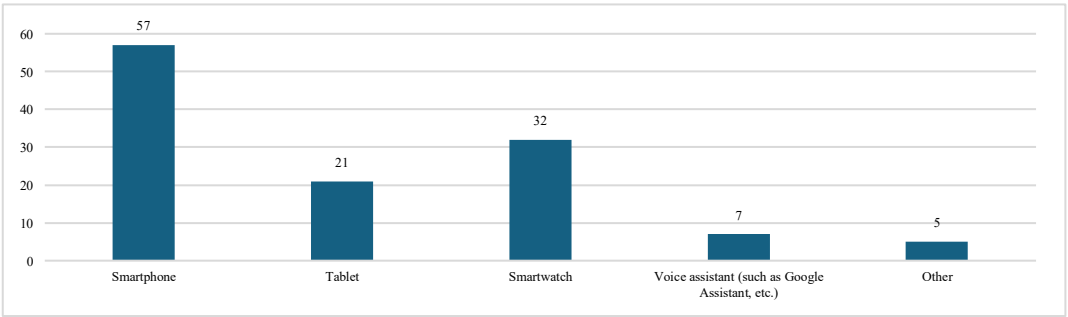

Figure 3: IoT devices often used by respondents for financial transactions

DOI: 10.54254/2754-1169/171/2025.21861

In the survey, 57 respondents (88%) often used smartphones for financial transactions, followed by smartwatches (32, 49%) and tablets (21, 32%). Only seven respondents (11%) often used voice assistants (such as Google Assistant, etc.) and other IoT devices (see Figure 3).

To sum up, most respondents were aged 18-35 years old, used PayPal very frequently, and often used smartphones and smartwatches for financial transactions.

4.2. IoT's impact on PayPal's payment systems

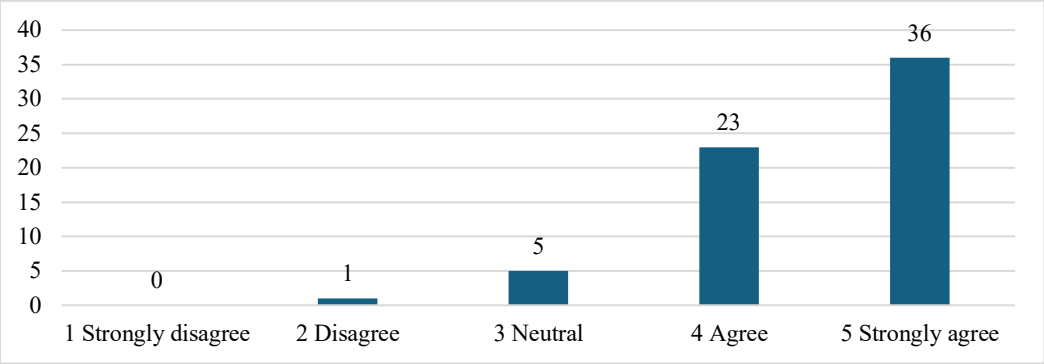

Figure 4: Transaction convenience of PayPal's IoT contactless payment

Figure 4 shows that 59 respondents (91%) agreed or strongly agreed that PayPal's contactless payment via smartphone and other IoT devices makes transactions more convenient. Meanwhile, 5 participants (8%) had a neutral perception of this statement. Only one respondent disagreed with this statement. This means that most respondents recognised the transaction convenience of PayPal's IoT contactless payment. As displayed in Figure 5, 40 respondents (62%) agreed or strongly agreed that voice payment through smart home devices (such as PayPal payment through Alexa, etc.) is very useful, while 7 respondents (10%) had the opposite perception. Meanwhile, 18 respondents (28%) had a neutral perception. This indicates that over 60% of respondents recognised the usefulness of voice payment through smart home devices.

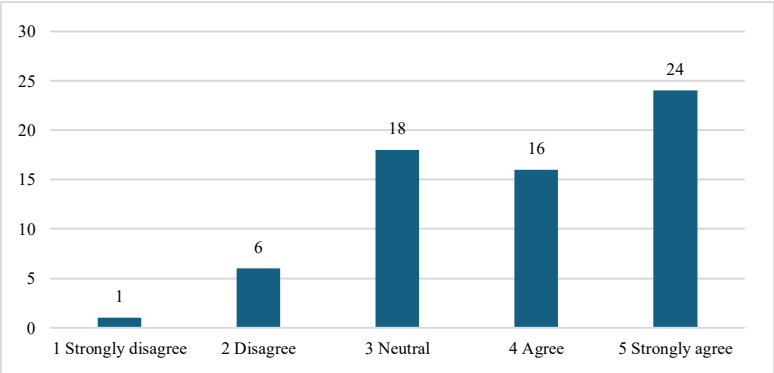

Figure 5: Usefulness of voice payment through smart home devices

DOI: 10.54254/2754-1169/171/2025.21861

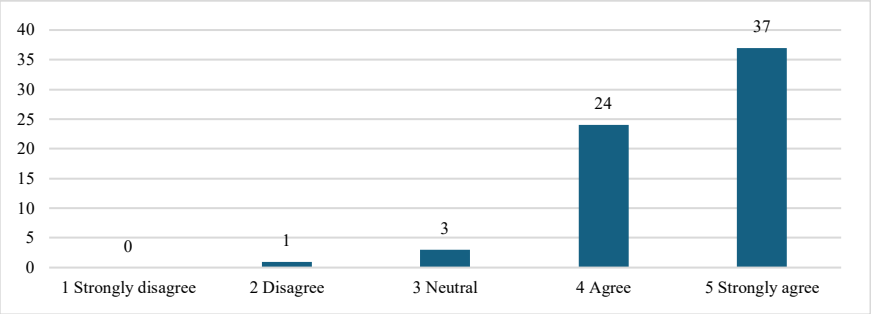

Figure 6: Time-saving of PayPal's automatic payment function through IoT devices

According to Figure 6, 61 respondents (94%) agreed or strongly agreed that v PayPal's automatic payment function through IoT devices saves the time in regular transactions, while only 4 respondents (6%) had different perceptions of it.

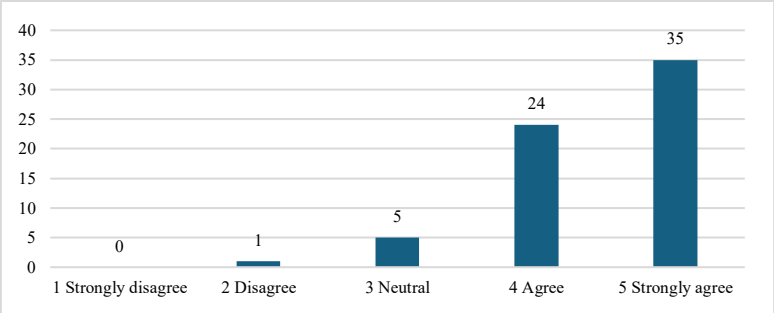

Figure 7: Seamless payment experience brought by PayPal's integration with various IoT devices

As can be seen from Figure 8, 59 respondents (91%) agreed or strongly agreed that PayPal's integration with various IoT devices offers a seamless payment experience, while only 6 respondents (9%) had different perceptions of this statement. Generally, the above findings show that most respondents recognised IoT's positive impacts on PayPal's payment system.

4.3. The security of PayPal's IoT payment system

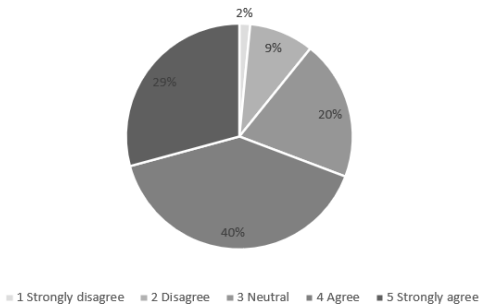

Figure 8: Security of PayPal's biometric authentication

As presented in Figure 8, 45 respondents (69%) agreed or strongly agreed that PayPal's biometric authentication (fingerprint/facial recognition) offers better security than traditional passwords, while 7 respondents (11%) disagreed or strongly disagreed with this view. At the same time, 13 respondents (20%) held a neutral view of it.

DOI: 10.54254/2754-1169/171/2025.21861

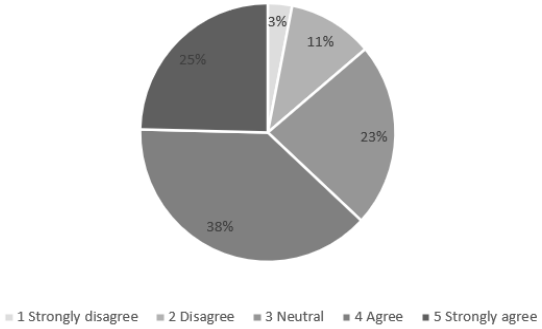

Figure 9: Security of payments through IoT devices connected to PayPal

As can be seen from Figure 9, 41 respondents (63%) agreed or strongly agreed that they feel secure when they make payments through IoT devices connected to PayPal, but 9 respondents (14%) disagreed or strongly disagreed with this statement. Meanwhile, there were still 15 respondents (23%) holding a neutral view view of it.

In the survey, 59 respondents (91%) agreed or strongly agreed that PayPal's real-time fraud detection system can effectively prevent unauthorised transactions. Meanwhile, only 6 respondents (9%) had the neutral or opposite view of this statement (see Figure 10).

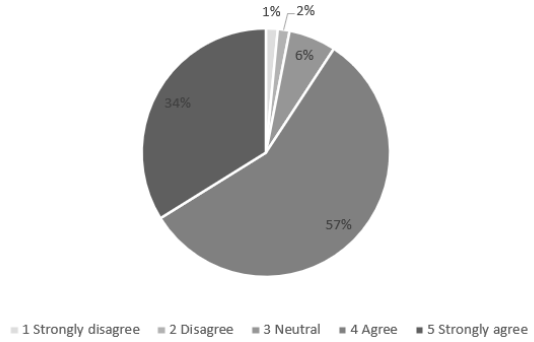

Figure 10: Security of PayPal's real-time fraud detection system

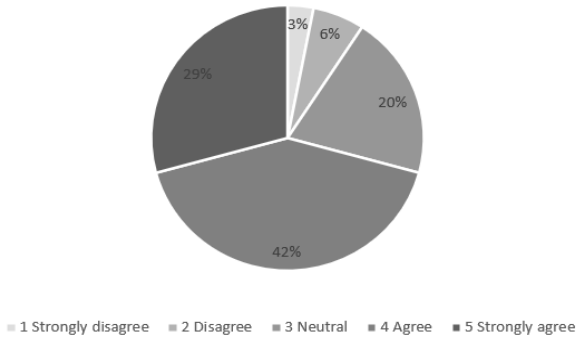

Figure 11: Security of PayPal's multi-layer security approach to IoT transactions

As shown in Figure 11, 46 respondents (69%) agreed or strongly agreed that PayPal's multi-layer security approach to IoT transactions gives them confidence in using IoT services. At the same time, 13 respondents (20%) had the neutral view of this statement. However, it should be seen that 6 respondents (9%) disagreed or strongly disagreed with it.

DOI: 10.54254/2754-1169/171/2025.21861

4.4. Challenges of PayPal's IoT integration into fintech

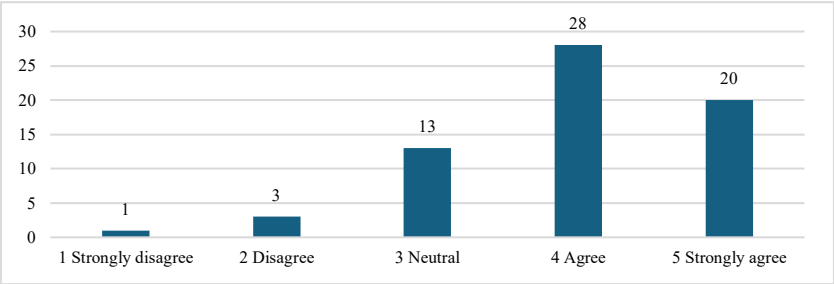

Figure 12: Data privacy concerns when using PayPal through IoT devices

In the survey, 48 respondents (74%) agreed or strongly agreed that when using PayPal through IoT devices, they are worried about their data privacy. Meanwhile, 13 respondents (20%) and 4 respondents (6%) had the neutral or opposite view of this statement (see Figure 12).

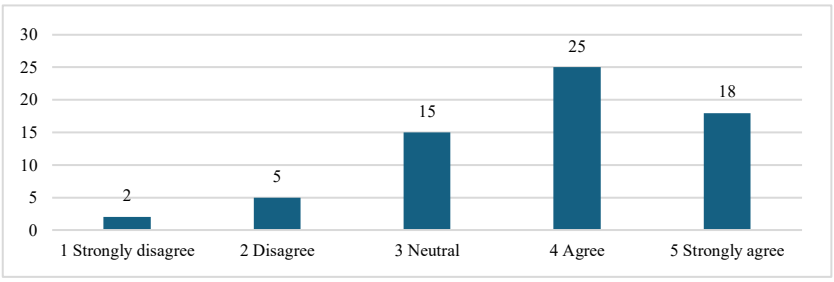

Figure 13: Concerns about unauthorised access to PayPal accounts

As shown in Figure 13, 43 respondents (66%) agreed or strongly agreed that they are concerned about unauthorised access to their PayPal accounts through networked IoT devices. At the same time, 15 respondents (23%) held the neutral view of the statement. Whereas, there were still 7 respondents (11%) who disagreed or strongly disagreed with the statement.

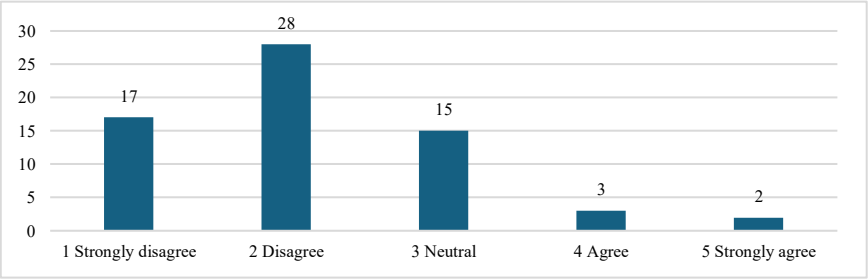

Figure 14: Technical problems when using PayPal on different IoT devices

45 respondents (69%) disagreed or strongly disagreed that they sometimes encounter technical problems when using PayPal on different IoT devices, while only 5 respondents (8%) held the opposite view of this statement. Additionally, 15 respondents (23%) held the neutral view of the statement (see Figure 14). This means that technical problems are not a major challenge of PayPal's IoT integration into fintech.

As presented in Figure 15, 43 respondents (66%) disagreed or strongly disagreed that they are worried about the compatibility issues between PayPal and different IoT devices, but only 6 respondents (9%) had the opposite view of the statement. In addition, there were 16 respondents (25%)

DOI: 10.54254/2754-1169/171/2025.21861

holding the neutral view of the statement. This indicates that compatibility issues between PayPal and different IoT devices are not a major challenge of PayPal's IoT integration into fintech.

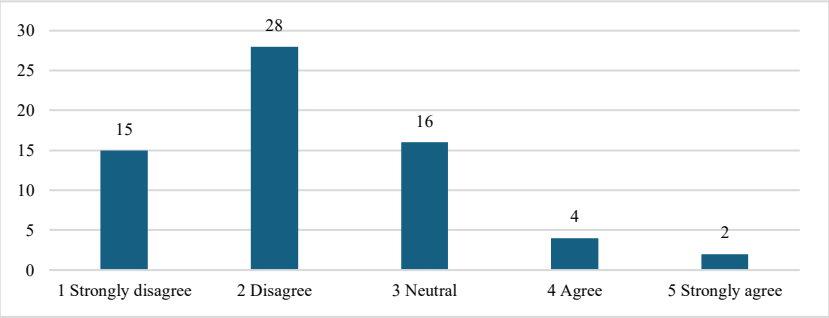

Figure 15: Compatibility issues between PayPal and different IoT devices

4.5. Discussion

The findings of this study both conform to and extend existing literature on the integration of IoT into fintech payment systems and security. By using PayPal as a case study, this study provides empirical evidence on IoT's transformative potential in enhancing transaction efficiency, user convenience, and financial security. The survey findings indicated that most respondents perceived that PayPal's IoT-enabled functions (such as automatic transactions, contactless payment, etc.) are very convenient and time-saving. The findings once again confirmed Gujral's[9] research that the integration of IoT improves the convenience of users through personalisation and high efficiency. Likewise, PayPal users' high acceptance of voice payments demonstrated in this study also supports the IoT to change financial interactions through smart speakers and other innovative interfaces [15].

Beyond enhancing payment systems, IoT also plays a pivotal role in addressing financial security, although it presents its own set of challenges. Regarding security, this study emphasised that respondents believed that biometric authentication and PayPal's real-time fraud detection system are effective measures to prevent unauthorised transactions. The findings are in line with Hussein's [10] results that the IoT biometric systems can greatly decrease the risks of identity theft and fraud. In addition, the positive feedback on PayPal's multi-layered security approach is consistent with the studies on the use of encryption and blockchain technology to strengthen data security [13].

However, the benefits of IoT integration are not without trade-offs. Key challenges, such as privacy concerns and user trust, remain critical issues for both PayPal and the wider fintech ecosystem. This aligned with Kshetri's [2] view that the IoT tends to increase the vulnerability of privacy leakage. Technical and compatibility issues were not the main concerns of PayPal users, but this was in stark contrast to Patel et al.'s [14] survey results that interoperability is a major obstacle to the integration of the IoT. In short, although the IoT has greatly strengthened the fintech system, solving privacy issues and enhancing user trust are still the main priorities of PayPal and even the fintech industry.

5. Conclusion

Taking PayPal as a single case, this study explored the IoT integration into fintech, focusing on studying the IoT's impacts on payment systems and security. This made contributions to the increasing research on the IoT integration into fintech, and offered useful inspiration for fintech companies, regulators and policymakers to optimise the application of the IoT in financial services. This study argued that IoT can greatly enhance PayPal's payment ecosystem by means of the improvement of user convenience, automated payments, as well as seamless and contactless transactions. Additionally, biometric authentication that is enabled by IoT can largely reduce unauthorised access; and PayPal's advanced real-time fraud detection system can significantly reduce

DOI: 10.54254/2754-1169/171/2025.21861

fraudulent transactions and enhance financial security. But meanwhile, the challenges of integrating IoT into fintech did exist, mainly including data privacy issues and concerns about unauthorised access. These challenges reveal the need for industry-wide collaboration on standards and protocols.

Although this study provided valuable insights, it also has limitations for the following reasons. First, this study only focused on a single case with PayPal as the focus; and the findings may not fully generalise to the entire financial industry. Second, the small sample size (65) in Australia may not well represent the global PayPal user base, which could restrict the generalisability of the research findings. Third, given the rapid development of IoT and fintech, some of the findings and technologies discussed in this study may face timeliness challenges, making ongoing research necessary. Therefore, these limitations should be considered when interpreting and applying the findings of this study. In the future, it is recommended that relevant studies involve more comparative cases of financial institutions to gain a more comprehensive understanding of IoT integration into fintech. In addition, future research is recommended to investigate 300-500 PayPal users worldwide to improve the samples' representativeness and generalisability of findings. Finally, research exploring the potential of emerging technologies (such as AI, edge computing, etc.) with IoT in financial services may also provide new insights into future trends in fintech.

References

[1] *PayPal. Annual Reports [Internet]. 2023. Available from: https://investor.pypl.com/financials/annual-reports/default.aspx*

[2] *Kshetri N. The economics of the Internet of Things in the Global South. Third World Quarterly. 2017; 38(2):311-339. Available from: https://doi.org/10.1080/01436597.2016.1191942*

[3] *Bagria VK, Meena B. Analysis of FinTech Enablers and Role of Future Internet of Things (IoT) in the New-Age Business World. International Journal of Management and Development Studies. 2023; 12(7):29-37. Available from: https://doi.org/10.53983/ijmds.v12n07.004*

[4] *Dange S. Secure Share: Optimal Blockchain Integration in IoT Systems. Journal of Computer Information Systems. 2024; 64(2):265-277. Available from: https://doi.org/10.1080/08874417.2023.2193943*

[5] *Maiti M, Ghosh U. Next Generation Internet of Things in Fintech Ecosystem. IEEE Internet of Things Journal. 2023; 10(3):2104-2111. Available from: https://doi.org/10.1109/JIOT.2021.3063494*

[6] *AL-Tamimi S, Al-Haija QA. Secure Mobile Payment (SMP): Challenges and Potential Solutions. International Journal of Intelligent Systems and Applications in Engineering. 2024; 12(11s):103-120. Available from: https://ijisae.org/index.php/IJISAE/article/view/4425*

[7] *Gkonis PK, Giannopoulos A, Panagiotis T, Masip-Bruin X, D'Andria F. A Survey on IoT-Edge-Cloud Continuum Systems: Status, Challenges, Use Cases, and Open Issues. Future Internet. 2023; 15(12): 383. Available from: https://doi.org/10.3390/fi15120383*

[8] *Allioui H, Mourdi, Y. Exploring the Full Potentials of IoT for Better Financial Growth and Stability: A Comprehensive Survey. MDPI. 2023; 23(19):8015. Available from: https://doi.org/10.3390/s23198015*

[9] *Gujral RK. Determinants of FinTech and Internet of Things for Technological Disruption: A New-Age Sustainable and Comprehensive Outlook. RESEARCH REVIEW International Journal of Multidisciplinary. 2023; 8(3):141-149. Available from: https://doi.org/10.31305/rrijm.2023.v08.n03.016*

[10] *Hussein O. Detection of Integrity Attacks on Permissions of Android-Based Mobile Apps: Security Evaluation on PayPal. IJCI International Journal of Computers and Information. 2024; 11(2):25-43. Available from: https://doi.org/10.21608/ijci.2024.277929.1156*

[11] *Fernández-Caramés TM, Fraga-Lamas P. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. IEEE Access. 2020; 8:21091-21116. Available from: https://doi.org/10.1109/ACCESS.2020.2968985*

[12] *Fazel E, Nezhad MZ, Rezazadeh J, Moradi M, Ayoade J. IoT convergence with machine learning & blockchain: A review. Internet of Things. 2024; 26:101187. Available from: https://doi.org/10.1016/j.iot.2024.101187*

[13] *Lu SY. An Analysis of the PayPals Corporate Strategy for Success. Advances in Economics Management and Political Sciences. 2023; 24(1):93-97. Available from: https://doi.org/10.54254/2754-1169/24/20230421*

[14] *Patel C, Doshi N. LDA-IoT: a level dependent authentication for IoT paradigm. Information Security Journal: A Global Perspective. 2021; 31(6):629-656. Available from: https://doi.org/10.1080/19393555.2021.1931573*

DOI: 10.54254/2754-1169/171/2025.21861

[15] *Dafri W, Al-Qaruty R. Challenges and opportunities to enhance digital financial transformation in crisis management. Social Sciences & Humanities Open. 2023; 8(1):100662. Available from: https://doi.org/10.1016/j.ssaho.2023.100662*
[16] *Bell E, Bryman A, Harley B. Business Research Methods. 6th ed. Oxford: Oxford University Press; 2022.*
[17] *Saunders MN, Lewis P. Doing Research in Business and Management: An Essential Guide to Planning Your Project. 3rd ed. London: Pearson; 2023.*
[18] *Kumar R. Research Methodology: A Step-by-Step Guide for Beginners. 6th ed. London: SAGE Publications; 2023.*
[19] *Ball HL. Conducting Online Surveys. Journal of Human Lactation. 2019; 35(3):413-417. Available from: https://doi.org/10.1177/0890334419848734*