Case Studies of Cybersecurity Implementation in Leading Digital Payment Platforms

Zheng Shuyu

Obuda University, Keleti Karoly faculty of Business and Management, Budapest, Hungary, zhengshuyu@stud.uni-obuda.hu

Andrea Tick

Obuda University, Keleti Karoly faculty of Business and Management, Budapest, Hungary, tick.andrea@kgk.uni-obuda.hu

Abstract: This study explores the impact of cybersecurity on digital payments, specifically examining how cyberattacks affect these systems. Using a case study approach and analyzing existing cybersecurity reports and academic research, the study reveals that while platforms like Alibaba and Revolut employ robust security measures like encryption and access control, they still struggle to effectively counter cyber threats. The research highlights the crucial role of both technological solutions and ongoing user education in strengthening digital payment security. These findings offer insights into digital payment platforms seeking to improve their cybersecurity strategies and user engagement to ensure transaction security and reliability. However, the reliance on publicly available data and literature may limit the study's scope, as it may not capture the full range of unpublished cybersecurity challenges faced by these platforms.

Keywords: Alibaba, Cyberattacks, Cybersecurity Strategies, Digital Payment, Revolut, Network Security, User Behavior

1 Introduction

Digital payments have become a crucial component of international economic activity in the current era of fast digitalization, considerably improving people's daily lives. The trend toward digitalization and the usage of the internet has resulted in significant changes to how the global economy runs. The introduction of a diverse set of financial technology (FinTech) applications allows users to go beyond the traditional cash-based payment method [1]. Digital payments are becoming increasingly common in people's daily lives. These rapid advancements in the financial sector resulted in the invention of numerous digital payment systems,

which enable payers and payees to send and receive money using digital apps. Thus, the payment system is rapidly transitioning from coin-based and paper-based money to digital forms of payments that are convenient, quick, and cost-effective [2].

However, worries about this payment method's security are growing along with its popularity. Cyber attackers constantly search for ways to breach the security defenses of digital payment systems in order to obtain, alter, or even destroy crucial data, posing a serious threat to personal privacy and property security. These tactics include malware, ransomware, phishing attacks, and more sophisticated persistent threats [3] These security risks can jeopardize the stability of the world economy in addition to undermining users' confidence in digital payment systems.

The majority of cyber-attacks are automated and aim to exploit common faults rather than specific websites or enterprises. It is a fallacy to assume that cyber attackers do not care about you. Every person who uses the internet needs cyber security. Ensuring secure payment is a crucial part of cyber security for any firm that accepts electronic payments or transactions [4].

Digital payments utilize a network of interconnected systems that ensure that transactions are executed swiftly. Cybersecurity is the core magnet holding all these systems together and ensuring that all these systems perform their duties without harm or malfunction. Figure 1 depicts how cyber security acts as the centerpiece connecting all the techniques used in the protection of digital payments.

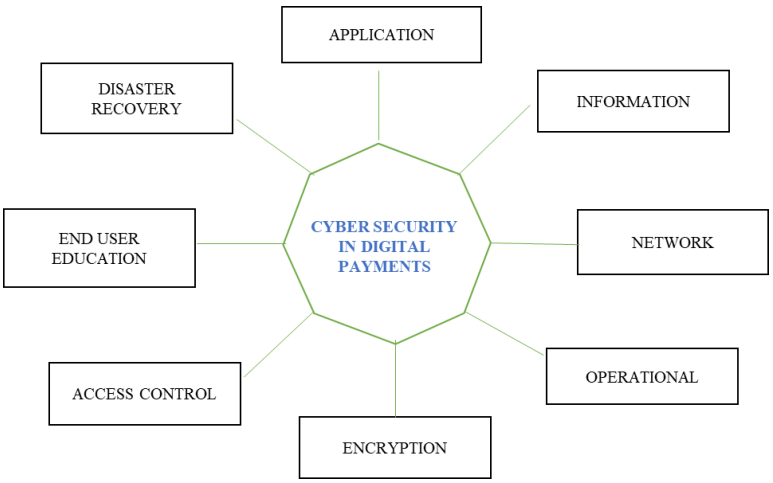

Figure 1.
A schematic diagram of the techniques employed by cyber security as protective tools to curb the surge of internal and external cybercrimes [5]

Cybersecurity is used to complete one or more successful transfers and prohibit undesired attacks that may or can happen. A few key figures in digital payments, their platforms, and the ways in which they have altered the overall landscape of retail will be focused on [6].

The purpose of this study is to explore the impact of cyber security incidents on the security of digital payment systems, user trust and willingness to use, as well as the effect of different cyber security measures on enhancing user trust and the stability of payment platforms. In order to determine the most effective cybersecurity strategies and measures in the current, constantly evolving cyber threat environment, the study focuses on analyzing which types of cybersecurity incidents have the greatest impact on digital payments and how different cybersecurity strategies shape users' trust in digital payment platforms.

The core research question posed in this study includes aims to understand what cybersecurity strategies and measures have been implemented by digital payment platforms. It looks at how effective these measures are in mitigating cyber threats and also understanding how cybersecurity incidents affected digital payment transaction volumes and user behavior. This study proposes the following research probe:

RP: Users with a high level of cybersecurity awareness are more likely to adopt digital payment methods, however they are still most likely to be the susceptible one to cyber-attacks [7].

Some of the most prevalent digital payments that are susceptible to cyber-attacks include, but are not limited to:

- Bank Transfer
- E-Wallet: Apple Pay
- Contactless payments: NFC
- Mobile POS
- QR codes
- Biometric authentication: Fingerprint,
- Wire Transfer
- P2P
- Direct Carrier Billing (DCB)
- Cryptocurrency Payments: Bitcoin

This study adopts a quantitative research methodology that relies heavily on secondary data sources such as publicly released cybersecurity news, reports and academic articles for systematic analysis. This approach not only helps to gain a deeper understanding of the multidimensional characteristics of the impact of cybersecurity incidents on digital payments but also provides a solid theoretical and practical foundation for making targeted security enhancement recommendations.

In summary, this research intends to improve user trust, protect the stability of the payment system, and support the robust growth of the digital economy by thoroughly examining cybersecurity events and their effects on digital payments. To conclude, it will offer actionable security strategy recommendations for digital payment which focus on Alibaba platforms.

This paper explores cybersecurity challenges in digital payments, focusing on the security measures of Alibaba and Revolut. First, the introduction section outlines the security threats facing digital payments and the research objectives; the literature review reviews the main types of cyberattacks and the strategies to counter them; the methodology describes the quantitative research methodology used and the data sources; the results section demonstrates the specific security measures of Alibaba and Revolut in terms of encryption, access control, and so on, and compares the security of the two; and the discussion analyses these measures and their impact on user trust; finally, the conclusion summarizes the findings, points out the limitations of the study and suggests directions for future research.

2 Literature Review

Previous research has revealed a broad understanding of cybersecurity challenges in the digital age, highlighting the escalation of sophisticated cyber threats such as malware, ransomware, phishing attacks, and advanced persistent threats (APTs) [8], [9]. The integration of AI and ML technologies is considered a revolutionary approach to combating these threats, enhancing anomaly detection, threat intelligence, predictive analytics, and behavioral analysis [10], [11].

Verma [12] highlights the accelerating pace of digital transformation, emphasizing that it brings with it both unparalleled efficiencies and extensive cybersecurity challenges. The digital age brings with it complex issues such as data breaches, ransomware and IoT vulnerabilities that need to be examined with vigilance [4]. Maurer & Nelson [13] noted that financial institutions play a key role in the economy, providing loans, savings, deposits, and ensuring that payments and settlements are conducted efficiently. Because of their critical role in the economy, these institutions face a significant risk from cyberattacks that could have a profound impact on the global economy.

While the convenience of digital payment systems is attracting more and more users, the corresponding lack of digital regulation and the absence of effective complaints and remedies have become a major pain point. This situation has emboldened cyber attackers, leading to more frequent security threats and financial losses for users [12].

The literature review highlights the dynamic and complex nature of cyber threats and the need for advanced and flexible defense mechanisms. Several studies have emphasized the critical role of artificial intelligence and machine learning in enhancing cybersecurity measures, and provided innovative strategies for threat detection, prediction, and incident response [8], [11], [12], [14], [15], [16]

The economy is moving toward digital transformation due to digital and business activities, and as technology advances, so do cyber threats and fraud. To achieve long-term revenue and cost optimization, some departments are able to optimize business operations independently thanks to big data, cloud computing, 3D printing, and cyber security [17]. Cyber threats escalated in the wake of COVID-19, highlighting the growing complexity and frequency of cybersecurity by discussing various attack channels such as social engineering and ransomware attacks [18] [19] alluded in the research, and elaborates on the security concerns of digital payment systems by highlighting consumer privacy and cybersecurity risks.

Gitau [20] hypothesized a significant relationship between cybersecurity awareness and e-market adoption, arguing that the higher the awareness, the higher the adoption rate. Trust in cybersecurity mechanisms is also expected to have a positive impact on adoption rates, as trust alleviates the fear of financial or data loss. The rapid growth in the field of digital payments can be traced back to a variety of factors, including the lack of user awareness of digital payment technologies and the inadequacy of digital payment infrastructure [12].

This viewpoint raises an important hypothesis that by gaining a deeper understanding of the specific causes of cyber-attacks during digital payments, the threats faced, and the possible strategies to address them, we can effectively improve our ability to prevent such cyber-attacks. The increase in cyber threats to financial institutions is being targeted by hackers both because of their increased digitization and their importance to the economy. The study argues that distributed ledger technology (DLT) can effectively defend against cyber-attacks because of its security. Maintaining global financial security requires governments, technology, and the financial sector to work together to develop a comprehensive strategy focused on developing effective measures to prevent, respond to, and mitigate cyber attacks [18]. While the consensus of these studies highlights the benefits of AI and machine learning in cybersecurity, they also note the challenges and ethical considerations of algorithmic bias, data privacy, and the adaptability of AI models to evolving threats. A limitation that recurs in these studies is that the rapid evolution of cyberthreats outpaces current defenses. The ethical implications and potential biases in AI-driven cybersecurity solutions also pose significant challenges that require a careful and ethical approach to technology implementation [11], [21]

3 Research Design and Research Methodology

This study aims to explore in depth the connectivity of cyber-attacks and their impact on digital payment systems, with a particular focus on how these attacks evolve into different types of threats. By analyzing emerging threats, technological advances, and user behavior in the digital attack environment, this study will identify potential vulnerabilities in digital systems and explore how financial institutions can enhance their resilience and security against attacks by implementing effective mitigation strategies.

The study employs an Okoli and Schabram inspired 8-step guideline for conducting a schematic review of information from secondary research into interpretable review that researchers could use (Figure 2).

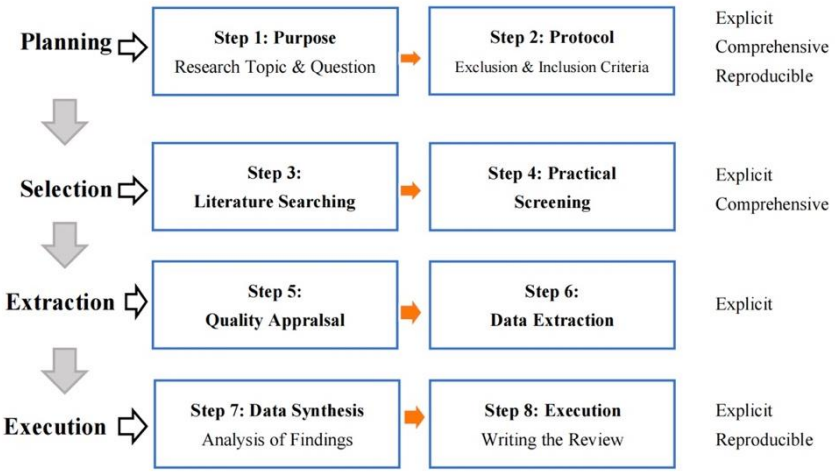

Figure 2.
Schematic 8-Step Review Process for analyzing secondary data [22], [23]

Figure 2 presents a schematic 8-step review process for analyzing secondary data. The process is divided into four major phases: Planning, Selection, Extraction, and Execution. The process is explicit, comprehensive, and reproducible, ensuring a transparent and systematic approach to secondary data analysis.

Step 1: *Purpose* – The goal of this study was to combine available empirical knowledge about the rise of cyber security in digital payments with a zoom in on Alibaba's web platform.

Step 2: *Protocol* – Predefined eligibility criteria were established prior to the initial 'search procedure' (step 3). The protocol comprises of 'inclusion and exclusion' criteria. The articles that meet the delimitation criteria are to be included for the

review (e.g., articles written in English, published journal articles and conference proceedings), while articles written in languages other than English, research in progress, or 'articles in press' are to be excluded based on the criteria set.

The study solely contains empirical studies, thus conceptual papers like literature reviews and book chapters will be eliminated. However, the insights gained from these papers are included in the study's theoretical framework.

Step 3: *Literature Search* – This phase depicts the search method and first selection of papers, including the keywords and databases utilized, the delimitation criteria specified above, and the number of articles discovered throughout the search process. The major database searched was 'Scopus' using the required keywords, download bibliographic data and author data from Scopus to be able to run analytics on Alibaba's critical cybersecurity issues. In the line diagram of the VOSviewer, the main Alibaba network safety is based around ‘network security, ‘cloud computing’, ‘security systems information management’, ‘virtual machine’, ‘electronic commerce’ as the main important words to analyze. Only peer-reviewed scholarly articles from journals and conferences were considered, as specified in step 2 (protocol), with no date constraints. The search was not limited by date because, while the field of study is expanding and digital payment systems are fast evolving to meet new difficulties, there is a scarcity of relevant empirical studies on this overall topic.

Step 4: *Practical Screen* – After the practical from Scopus download everything together with bibliographic data and author data to be able to run an analysis by country.

Step 5: *Quality Screen* – The suitable articles chosen in the previous step were then vetted for quality by carefully reading the whole text of each item. Because only empirical papers were included in this study to assure the quality of the review, the quality screening focused on the methodological validity and reliability of the findings.

Step 6: *Data Extraction* – having completed the quality screening, data was extracted to specifically address the first research question. This then allowed for the second question to be answered.

Step 7: *Data Synthesis* – In this section, the extracted data is arranged and analyzed to compare Alibaba in an organized fashion to assist in defining the broad topic of the effects of cyber security in digital payments.

Step 8: *Writing the Review* – The last seven steps clearly document the review technique for easy replication. The authors cooperatively refined the report,

focusing on concise, clear descriptions to enhance readability and distribution potential.

Moreover, the present study is designed to be replicable. The data and research models are clearly presented so that other researchers can understand and replicate these methods and results. This contributes to the ongoing dialogue and development within the cybersecurity community regarding digital payments in VOSviewer.

4 Results

In the digital era, cybersecurity has become a key component of technological innovation. This research explores the performance of Alibaba and e-payment applications such as Revolut in some different areas through a comparative analysis in application security; disaster recovery; end-user education; assess control and network operation. This comparison aims to reveal the differences in strategy and effectiveness of different platforms in handing security challenges that provide insights into cybersecurity practices.

4.1 Alibaba VOSviewer analysis

In order to comprehensively analyse the progress of Alibaba's research on cybersecurity, relevant literature can be downloaded from the Scopus database.

Firstly, by filtering keywords such as ‘Alibaba’, ‘cyber security’, ‘cloud computing’ and ‘data protection’, we locate specific research papers. and ‘data protection’, etc., to locate specific research papers. Then, the results are further refined by using the two dimensions of authors and domains of the literature. Through this method, high-quality literature related to Alibaba cybersecurity can be obtained. Keyword network analysis of the downloaded literature can be performed using VOSviewer software. This analysis can help reveal the correlations and research trends between different research topics. As shown in Figure 3, the network connections between keywords and the size of the nodes can visualise which areas are the hotspots of research and how different topics are related to each other. For example, it can be seen that keywords such as ‘cloud services’, ‘data security’ and ‘machine learning’ occupy a central position in the network, indicating that these areas are the current research focuses of cybersecurity. In this way, researchers can effectively grasp Alibaba's research dynamics and core technologies in the field of cybersecurity, providing theoretical support and technical guidance for further research and application.

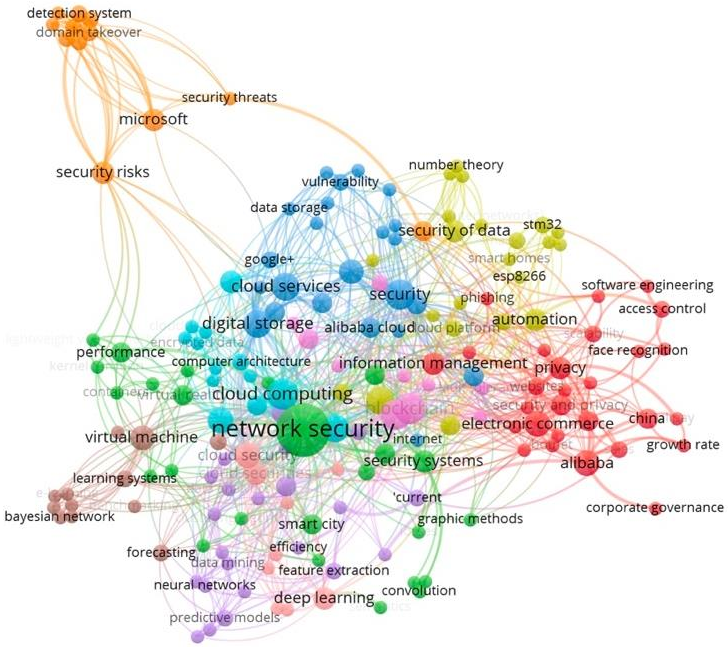

Figure 3.

Cybersecurity links to Alibaba's web platform, source: VOSviewer by sources from Scopus, 2024

Figure 3 shows that 'network security' is at the center of the knowledge graph and is closely linked to a number of technologies and concepts, such as 'cloud computing security' and 'block chain', demonstrating its position at the heart of protecting information systems. Cloud services such as 'Google+' and 'Alibaba Cloud Platform' are closely related to cybersecurity, reflecting the importance of infrastructure and platform support in modern cybersecurity. In addition, the linkage of 'data security' with concepts such as 'data storage' and 'privacy' underscores the importance of protecting data in the cyberenvironment, which is not only a technical issue, but is also closely related to regulatory compliance and user privacy protection [24]. Table 1 lists the most frequent keywords and their link strength.

Based on the analysis of keyword frequencies from Table 1, the important concerns about Alibaba in the field of cybersecurity. These high-frequency terms reflect Alibaba's multi-dimensional layout of security technologies and services, especially its investment in network cybersecurity, blockchain, cloud services, cryptography, digital storage, internet of things, alibaba, cloud security, cloud-computing, electronic commerce, cloud platforms and virtual machine.

Keyword	Occurrences	Total link strength
network security	29	172
blockchain	19	65
security	9	45
cloud service	8	67
cryptography	8	66
digital storage	8	41
Internet of things	8	60
alibaba	7	18
Cloud security	7	67
Cloud-computing	7	51
Electronic commerce	7	29
Cloud platforms	6	46
Virtual machine	6	49

Table 1.

Main keywords from VOSviewer

Firstly, ‘network security’ and ‘security’ show that Alibaba attaches great importance to overall network security and is closely linked to cloud computing, virtual machines and other related technologies, which lay the foundation for the security of the e-commerce platform . In addition, ‘blockchain’, as an emerging technology, plays an important role in Alibaba's ecosystem, and the decentralised and tamper-proof nature of blockchain effectively improves the security of data transmission and storage, especially in the field of digital payment [25]. Secondly, the keywords ‘cloud service’, ‘cloud security’ and ‘cloud computing’ show Alibaba's security and protection strategy in cloud storage and processing [26]. As one of the world's leading cloud computing platforms, Alibaba continues to strengthen its security protection mechanisms in the cloud environment. Combined with ‘virtual machine’ technology, Alibaba is able to provide users with highly isolated computing resources, reducing the risk of cross-tenant attacks . Finally, the frequency of ‘e-commerce’ and ‘Alibaba’ suggests that Alibaba has spared no effort in securing e-commerce platforms for transaction security and user data protection, especially in the application of emerging technologies such as the ‘Internet of Things’ and ‘digital storage’, which have further raised security standards within its ecosystem [27], [28].

Encryption is an integral part of network security, and its connection to ‘performance’ and ‘digital storage’ illustrates the dual role of encryption in performance optimization and security enhancement.’ The connection to ‘performance’ and ‘digital storage’ illustrates the dual role of encryption in optimizing performance and increasing security. The mention of modern technologies such as ‘Smart Home’ and ‘Face Recognition’ shows that with technological advances, the security of the home and the individual is becoming more and more important and raises new issues of privacy and data protection.

Major technology companies such as "Alibaba," "Microsoft," and "Google" occupy prominent positions in the map, indicating their leadership roles in the global field of network security. These companies not only provide technical solutions but also play key roles in setting security standards and policies [28], [29], [30], [31]. Additionally, the special marking of "China" reflects the country's importance in the development of network security technology, policymaking, and market development, as well as its significant impact on the global network security ecosystem.

Terms like "phishing" and "domain takeover" in the map represent specific threats faced in network security, which require particular techniques and strategies to counter. The construction of ‘security systems and the management of ‘security risks’ were highlighted as important components of cybersecurity that need to be maintained through continuous evaluation and updating.

The application of ‘deep learning’ and ‘data mining’ technologies in network security is mainly reflected in the use of big data analysis to predict and identify potential threats. The use of deep learning technology not only improves the automation level of threat detection, but also enhances the efficiency of security incident processing, reflecting the key role of artificial intelligence technology in modern network security.

4.2 Comparison of applications

4.2.1 Application security

Alibaba Group has taken comprehensive measures in maintaining the security of its multi-platform applications, which include Linux, MacOS, iOS, Android and AliOS. The company has not only developed technologies for code obfuscation, anti-reversal and anti-tampering, but has also successfully implemented these technologies in critical business activities [26]. For example, during the Double 11 mega shopping festival, these technologies provided solid security for the transaction chain. In addition, in order to deal with online scalping and other unlawful behaviors, Alibaba has developed special protection features for 12306 APP (China Railway Customer Service Platform), which effectively stops illegal ticket-snatching behaviors.

In addition, the company also excels in the field of IoT security. Through in-depth research on various types of sensors and IoT systems, including firmware and software levels, Alibaba aims to uncover and patch potential security vulnerabilities. In particular, in the research of 4G/5G communication protocols and

baseband security, the company combines IoT virtualization technology to enhance the security performance of devices [32].

For vulnerability mining technology, Alibaba adopts two main approaches: first, through in-depth dynamic and static analysis, recording and analyzing program running state and behavioral data, assisting security personnel to quickly understand the program's potential attack paths; and second, implementing large-scale vulnerability mining, which combines expert experience with scaled and data-driven analysis to improve the efficiency and vulnerability discovery ability of security experts when faced with a large number of analytical objects. The ability of the security experts to find vulnerabilities. In the future direction of cooperation, the company is particularly looking forward to further research and develop in the automated verification of vulnerabilities and the application of machine learning in vulnerability mining scenarios, in order to continue to enhance the cutting-edge and effectiveness of application security technology [33].

4.2.2 Disaster recovery

First, the appropriate device is selected for operation through a well-defined workflow. Next, a new cloud provider is added and the necessary storage space information is obtained, a process that requires proper entry of authentication information to ensure access. The configuration of storage pools details how to select the appropriate RAID (Redundant Array of Independent Disks) level based on the storage requirements and name and configure the pools to ensure data security and access speed. Also covered is how to optimize the data writing process by selecting specific storage policies, such as the choice of write-back and write-through policies. Finally, a detailed description of how to set up and manage data volumes in disaster recovery, including restoring data from a selected Bucket, is presented. These steps exemplify the complexity and importance of implementing disaster recovery in modern cloud computing environments, providing organizations with an effective way to protect critical data and ensure business continuity [34].

4.2.3 Access control

Alibaba's access control system employs multi-level and multi-dimensional security measures to protect data and resources. This includes physical access control, network access control, and application and data level access control. Alibaba utilizes the latest technologies and strategies, such as the Least Privilege Principle, Role-Based Access Control (RBAC), Multi-Factor Authentication and continuous security auditing. These measures help ensure that only authorized users have access to sensitive information and critical systems, thereby reducing the risk of data leakage or unauthorized access [35].

4.2.4 Encryption

Alipay's key generation relies on self-developed security technology, which consists of two main parts: encryption algorithms and signature algorithms. In terms of encryption, Alipay utilizes advanced AES and RSA algorithms to encrypt users' payment passwords, ensuring the confidentiality and integrity of password data. For signature verification, SHA1 and SHA256 algorithms, which combine timestamp and hash value technologies, are used to strengthen the security and reliability of authentication [36], [37].

Alipay's key management process includes three links: key generation, storage and use. In the generation session, keys are generated under strict control through a secure certification authority to meet high security standards. In the storage segment, the keys are securely stored in a professional data center under the strict supervision of professional security managers to prevent any unauthorized access or leakage. In the use segment, Alipay closely verifies the payment passwords entered by users to ensure the security of each payment behavior [36], [38]

In addition, Alipay implements multiple security measures, including encrypted processing of keys and double authentication technology, as well as backup and encrypted processing of data, to protect the security of user data in all aspects. Through these comprehensive measures, Alipay has demonstrated a high degree of responsibility and technical expertise in protecting user payment security, ensuring a safe and secure payment environment [39].

4.2.5 Privacy Information Protection

Alipay's Privacy Policy details how user information is handled, ensuring that collection and use are based on the principles of lawfulness, necessity and propriety. The policy includes detailed provisions on the collection, use, storage and sharing of information, and highlights users' rights to access and manage information, such as updating and managing privacy settings and account cancellation. It is specifically mentioned that if information needs to be shared with a third party, the legality and security measures of the third party will be strictly assessed. In addition, for minors' information, Alipay takes additional protection measures and makes it clear that users can change the scope of authorization or directly cancel their accounts through specific settings to ensure that they can effectively manage their personal information [40]

4.2.6 Network and Operational Issues

Alibaba's Chief Risk Officer [28] revealed the extensive measures Alibaba has taken to secure its vast network, which serves 670 million domestic shoppers and

130 million international customers. Zheng highlighted that Alibaba's systems fend off five billion cyberattacks a day, help 40 per cent of China's websites and patch 8.33 million vulnerabilities throughout the year. The company provides basic security defenses for more than one million businesses and handles more than half of the country's large-scale DDoS attacks.

Based on its 20 years of experience, Alibaba has developed a comprehensive 'end-to-end network security protection' system that can withstand terabyte-level attacks, with the largest attack being 776.8 GB. In addition, Alibaba ensures content security through an algorithmic recognition system that analyses text, images, videos and live broadcasts to eliminate harmful online information. information online. The 'Technology Brain for Intellectual Property Protection' has accumulated years of experience in developing from combating online infringement to protecting original designs [29].

5 Research Findings and Discussion

Fintech businesses are becoming more and more crucial in today's globalized economy by providing creative services and solutions to consumers varied financial demands. An overview of some of the most well-known fintech platforms and their featured services is provided below. These services range from online payments to money exchange, international remittances, and more, demonstrating how effective technology integration can further optimize and transform the financial services experience.

Both Alibaba and Revolut prioritize strong security to protect their users. Alibaba uses advanced encryption methods and a centralized key management system to secure transactions across its vast network. On the other hand, Revolut emphasizes end-to-end encryption, multi-factor authentication and real-time fraud detection, focusing on protecting user accounts and international transactions.

Aspect	Alibaba	Revolut
Focus	Online payments; Wealth management; Credit; Insurance.	Currency exchange; Online payment; International transfer;
Key Security Features	Advanced encryption; Centralized key management.	End-to-end encryption; single-use virtual card; real time fraud
Integration	Shopping payments; public service.	Mobile-first approach; innovative financial products
Technology	Incorporates advanced encryption methods; user-centric financial ecosystem.	Utilizes GPS for transaction verification; virtual cards; real-time fraud detection.
Unique Offerings	Focus on Chinese market; e-commerce	Cryptocurrency transactions
Innovation	To improve user experience, financial services are continuously integrated into their environment.	Consistent innovation with new financial products and data-driven personalized services
Preventing Fraud	focuses on transaction security and encryption	Sherlock anti-fraud system with real-time monitoring; alerts based on location and transaction behavior

Table 2.
Comparison between Alibaba and Revolut

Alibaba provides a comprehensive suite of financial services, including online payment, wealth management, credit services, and insurance [25], [41], [42]. It has seamlessly integrated into the daily lives of users, encompassing a wide range of activities from shopping payments to public service fee transactions, thereby constructing an extensive ecosystem. This strategic incorporation of advanced technological solutions not only reinforces Alipay's position in the financial services sector but also contributes to the evolution of a more sophisticated and user-centric financial ecosystem [27], [43]

Revolut delivers an expansive range of financial services, encompassing currency exchange, international transfers, debit card provisions, cryptocurrency transactions, and stock trading. Through ongoing innovation and the introduction of novel financial products, the platform caters to the diversified demands of its users. Additionally, Revolut employs sophisticated data analytics and personalized services to enhance the user experience and fulfill individualized requirements.

Revolut's mobile apps offer multiple authentication methods, including password protection and fingerprint recognition. These measures effectively prevent unauthorized access and ensure the security of user accounts, and Revolut's 'Sherlock' anti-fraud system monitors and detects suspicious activity in real time, enabling the security team to respond quickly to potential threats and protect user funds. To further enhance the security of online payments, Revolut offers a single-use virtual card. Users can destroy the card after completing an online transaction, avoiding the risk of secondary use of the card number. The Revolut app utilizes

GPS technology to track a user's geographic location in order to prevent suspicious transactions that are not made at commonly used locations. For example, if a user's mobile phone is located in the UK, but their Revolut card is being used in Spain, the system may refuse to perform the transaction [44], [45], [45], [46], [47].

Conclusion

This study systematically explores the dynamic and multifaceted impact of cybersecurity on digital payment systems, revealing vulnerabilities and robust defense mechanisms used to mitigate these risks. Through detailed analyses, primarily of the Alibaba platform, we identify key security measures such as encryption, access control, and disaster recovery as essential to protecting digital transactions. However, despite these advances, the ongoing evolution of cyberthreats continues to pose significant challenges that require continuous adaptation and improvement of security frameworks.

The main limitation of this study is its reliance on secondary data, which may not fully capture the rapidly changing cybersecurity threat and innovation landscape. In addition, the focus on specific digital payment platforms may not generalize to the wider fintech sector. Future research should aim to combine primary data collection and case studies to provide deeper insights into specific cybersecurity challenges and solutions.

Exploring the potential of emerging technologies such as artificial intelligence and machine learning for predictive threat detection is a promising direction. Further development may involve the creation of real-time security systems that can dynamically adapt to new threats as they emerge. Collaboration between financial institutions, technology providers and regulators are essential to create a resilient digital economy that can withstand the complex cyber threats of the future.

References

[1] N. N. Cele and S. Kwenda, “Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review,” J. Financ. Crime, Apr. 2024, doi: 10.1108/JFC-10-2023-0263.

[2] A. Premchand and A. Choudry, “Future of Payments- ePayments,” Int. J. Emerg. Technol. Adv. Eng., 5(1) pp. 110–114, 2015.

[3] J. Patil, “Cyber laws in india: an overview,” 2022, [Online]. Available: https://www.researchgate.net/publication/358797907_Cyber_Laws_in_India_An_Overview

[4] P. Anand, Y. Singh, A. Selwal, P. K. Singh, R. A. Felseghi, and M. S. Raboaca, “IoVT: Internet of Vulnerable Things? Threat Architecture, Attack Surfaces, and Vulnerabilities in Internet of Things and Its Applications

towards Smart Grids," Energies, 13(18) p. 4813, Sep. 2020, doi: 10.3390/en13184813.

[5] A. M. Sahi, H. Khalid, A. F. Abbas, K. Zedan, S. F. A. Khatib, and H. Al Amosh, "The Research Trend of Security and Privacy in Digital Payment," Informatics, 9(2) p. 32, Apr. 2022, doi: 10.3390/informatics9020032.

[6] Y. Guan and A. Tick, "Literature Review on Security of Personal Information in Electronic Payments," in 2024 IEEE 18th International Symposium on Applied Computational Intelligence and Informatics (SACI), Timisoara, Romania: IEEE, May 2024, pp. 000533–000540. doi: 10.1109/SACI60582.2024.10619864.

[7] A. Tick and P. T. Mai, "Cyber Security Awareness and the Behaviors of Higher Education Students, using Smartphones in Vietnam," Acta Polytech. Hung., 21(12) pp. 111–131, 2024, doi: 10.12700/APH.21.12.2024.12.7.

[8] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions," Electronics, 12(6) p. 1333, Mar. 2023, doi: 10.3390/electronics12061333.

[9] N. Sámson and A. Tick, "Digital Defense: Investigating Human Aspects of Cybersecurity," in 2024 IEEE 18th International Symposium on Applied Computational Intelligence and Informatics (SACI), Timisoara, Romania: IEEE, May 2024, pp. 000525–000532. doi: 10.1109/SACI60582.2024.10619840.

[10] D. Augustyn and A. Tick, "Security Threats in Online Metasearch Booking Services," in 2020 IEEE 20th International Symposium on Computational Intelligence and Informatics (CINTI), Budapest, Hungary: IEEE, Nov. 2020, pp. 000017–000022. doi: 10.1109/CINTI51262.2020.9305839.

[11] R. Evren and M. Smith, "The Cyber Threat Landscape: Understanding and Mitigating Risks," EasyChair Prepr., no. 11705, pp. 1–12, 2024.

[12] Verma, "20 cybersecurity challenges in the era of digital transformation," 1, 2024, doi: 10.25215/9392917848.20.

[13] T. Maurer and A. Nelson, "Cyber threats to the financial system are growing, and the global community must cooperate to protect it," Finance Dev., March 2021, pp. 24–27, 2021.

[14] H. A. A. Al-Hashemi, "Evaluating the role of artificial intelligence and machine learning technologies in developing and improving the quality of electronic financial disclosure," Am. J. Econ. Bus. Manag., 6(10) pp. 239–262, Oct. 2023, doi: 10.31150/ajebm.v6i10.2513.

[15] G. Nagar and A. Manoharan, "Understanding the Threat at Landscpe: A Comprehensive Analysis of Cyber-security Risks in 2024," Int. Res. J. Mod. Eng. Technol. Sci., 6(3), pp. 5706–5713, Jan. 2024.

[16] M. Waqas, S. Tu, Z. Halim, S. U. Rehman, G. Abbas, and Z. H. Abbas, “The role of artificial intelligence and machine learning in wireless networks security: principle, practice and challenges,” Artif. Intell. Rev., 55(7), pp. 5215–5261, 2022, doi: 10.1007/s10462-022-10143-2.

[17] O. C. Obi, S. O. Dawodu, A. I. Daraojimba, Shedrack Onwusinkwue `, O. V. Akagha, and I. A. I. Ahmad, “Rreview of Evolving Cloud Computing paradigms: Security, Efficiency, and Innovations,” Comput. Sci. IT Res. J., 5(2), Art. no. 2, 2024, doi: 10.51594/csitrj.v5i2.757.

[18] O. Gulyas and G. Kiss, “Impact of cyber-attacks on the financial institutions,” Procedia Comput. Sci., 219, pp. 84–90, 2023, doi: 10.1016/j.procs.2023.01.267.

[19] B. Udo, “Digital Payment Solutions: Consumer Privacy and Cybersecurity Concerns,” SSRN Electron. J., 2023, doi: 10.2139/ssrn.4345700.

[20] A. Gitau, “Impact of Cybersecurity of E-payments on Adoption of E-marketplaces among Private University Students in Kenya,” Africa: United States International University, 2021, p. 86. [Online]. Available: https://erepo.usiu.ac.ke/bitstream/handle/11732/6670/Gitau%20Angela%20MBA%202021.pdf?sequence=1&isAllowed=y

[21] CCICED, “Major Green Technology Innovation and Implementation Mechanism,” in Green Recovery with Resilience and High Quality Development, Singapore: Springer Nature Singapore, 2023, pp. 291–356. doi: 10.1007/978-981-19-9470-8_6.

[22] K. Khando, M. S. Islam, and S. Gao, “The Emerging Technologies of Digital Payments and Associated Challenges: A Systematic Literature Review,” Future Internet, 15(1) p. 21, 2022, doi: 10.3390/fi15010021.

[23] C. Okoli and K. Schabram, “A Guide to Conducting a Systematic Literature Review of Information Systems Research,” SSRN Electron. J., 2010, doi: 10.2139/ssrn.1954824.

[24] A. Ospanova, A. Zharkimbekova, L. Kussepova, A. Tokkuliyeva, and M. Kokkoz, “Cloud Service for Protecting Computer Networks of Enterprises Using Intelligent Hardware and Software Devices, Based on Raspberry Pi Microcomputers,” Acta Polytech. Hung., 19(4), pp. 85–103, 2022, doi: 10.12700/APH.19.4.2022.4.5.

[25] G. Srivastava, S. Kumar, and S. Priya, “Blockchain Enabled Secured Carpooling Platform with Proof of Concept,” in Emerging Electronics and Automation, vol. 1088, M. Gabbouj, S. S. Pandey, H. K. Garg, and R. Hazra, Eds., in Lecture Notes in Electrical Engineering, vol. 1088. , Singapore: Springer Nature Singapore, 2024, pp. 283–294. doi: 10.1007/978-981-99-6855-8_22.

[26] Nallathambi, “Alibaba Cloud in Cybersecurity.” 2023. [Online]. Available: https://www.alibabacloud.com/blog/alibaba-cloud-in-cybersecurity_600315

[27] W. Weng, “Alipay beats top global platforms in coverage, service and ecosystem bandwidth.” 2024. [Online]. Available: https://tabinsights.com/article/alipay-tops-the-best-platforms-ranking-in-2023

[28] J. Zheng, “How does Alibaba keep its network safe? Zheng Junfang, chief risk officer, answers the question.” 2019. [Online]. Available: https://finance.sina.cn/stock/relnews/us/2019-10-12/detail-iicezzrr1823568.d.html?oid=5_NBA2&vt=4&pos=102&cid=76524

[29] S. Alizila, “Alibaba IPR Report Demonstrates Brand-Protection Leadership.” 2020. [Online]. Available: https://www.alizila.com/alibaba-ipr-report-demonstrates-brand-protection-leadership/

[30] L. Wang, “Global network security governance trend and China’s practice,” Int. Cybersecurity Law Rev., 2(1), pp. 93–112, 2021, doi: 10.1365/s43439-021-00025-8.

[31] X. Zhou, Y. Sawada, M. Shum, and E. S. Tan, “COVID-19 containment policies, digitalization and sustainable development goals: evidence from Alibaba’s administrative data,” Humanit. Soc. Sci. Commun., 11(1), p. 75, Jan. 2024, doi: 10.1057/s41599-023-02547-4.

[32] S. Pirbhulal, S. Chockalingam, A. Shukla, and H. Abie, “IoT cybersecurity in 5G and beyond: a systematic literature review,” Int. J. Inf. Secur.,23(4), pp. 2827–2879, 2024, doi: 10.1007/s10207-024-00865-5.

[33] W. Chao et al., “An Android Application Vulnerability Mining Method Based On Static and Dynamic Analysis,” in 2020 IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC), Chongqing, China: IEEE, Jun. 2020, pp. 599–603. doi: 10.1109/ITOEC49072.2020.9141575.

[34] Alibaba, “Cloud Disaster Recovery,” Alibaba Cloud. 2022. [Online]. Available: https://www.alibabacloud.com/help/zh/hcs/cloud-disaster-recovery

[35] N. Vaideeswaran, “What is role-based access control (RBAC),” Role-Based Access Control (RBAC) Explained. 2025. [Online]. Available: https://www.crowdstrike.com/en-us/cybersecurity-101/identity-protection/role-based-access-control/

[36] Alibaba Cloud, “Alibaba encryption service mechanism.” 2024. [Online]. Available: https://www.alibabacloud.com/help/zh/hsm/developer-reference/mechanisms

[37] K. Venkata Ramana, G. V. Sai Supraja, and V. Hibare, "Hybrid Cryptosystem's Design with AES and SHA-1 Algorithms," in Innovations in Signal Processing and Embedded Systems, J. K. Mandal, M. Hinchey, and K. S. Rao, Eds., in Algorithms for Intelligent Systems. , Singapore: Springer Nature Singapore, 2023, pp. 65–75. doi: 10.1007/978-981-19-1669-4_7.

[38] Alibaba Cloud, "Key Management Service." 2023. [Online]. Available: https://www.alibabacloud.com/help/en/kms/key-management-service/support/overview-11

[39] L. Changzhao, "Research on Security Factors of Mobile Payment —— Taking Alipay, the leader of China's third party payment, as an example," Lisbon, Portugal: ISCTE Business School, 2018, p. 78. [Online]. Available: https://repositorio.iscte-iul.pt/bitstream/10071/17734/1/master_li_changzhao.pdf

[40] Alipay, "Alipay Privacy Policy update announcement." 2022. [Online]. Available: https://help.alipay.com/lab/help_detail.htm?help_id=201603467440

[41] H. Huang et al., "PVM: Efficient Shadow Paging for Deploying Secure Containers in Cloud-native Environment," in Proceedings of the 29th Symposium on Operating Systems Principles, Koblenz Germany: ACM, Oct. 2023, pp. 515–530. doi: 10.1145/3600006.3613158.

[42] N. I. Mahbub, Md. D. Hossain, S. Akhter, Md. I. Hossain, K. Jeong, and E.-N. Huh, "Robustness of Workload Forecasting Models in Cloud Data Centers: A White-Box Adversarial Attack Perspective," IEEE Access, vol. 12, pp. 55248–55263, 2024, doi: 10.1109/ACCESS.2024.3385863.

[43] M. Y. Zhang and P. Williamson, "The emergence of multiplatform ecosystems: insights from China's mobile payments system in overcoming bottlenecks to reach the mass market," Technol. Forecast. Soc. Change, vol. 173, p. 121128, Dec. 2021, doi: 10.1016/j.techfore.2021.121128.

[44] Jitaru Mădălina and A. Bodnar, "Security analysis -Revolut," 2021, doi: 10.13140/RG.2.2.33681.25440.

[45] D. Lihhatsov, "How Revolut's Sherlock AI saves its customers from fraud." 2019. [Online]. Available: https://techhq.com/2019/11/how-revoluts-sherlock-ai-saves-its-customers-from-fraud/

[46] M. Polasik, P. Widawski, and A. Lis, "Challenger bank as a new digital form of providing financial services to retail customers in the EU internal market," in The Digitalization of Financial Markets, 1st ed., London: Routledge, 2021, pp. 175–193. doi: 10.4324/9781003095354-10.

[47] L. Thompsett, "Revolut Launches AI Feature to Protect Against Card Scams." 2024. [Online]. Available: https://fintechmagazine.com/articles/revolut-launches-ai-feature-to-protect-against-card-scams