

Assessing Data Sharing Risk in Cross-Border Payment: Insights from Institutional Experts

Dian Prima Sari¹, Yudho Giri Sucahyo²

^{1,2}Faculty of Computer Science, Universitas Indonesia, Indonesia

Article Info

Article history:

Received Mar 25, 2026

Revised May 18, 2026

Accepted May 22, 2026

Keywords:

Cross-Border Payment

Fuzzy-Delphi

Data Sharing

Data Sovereignty

Information Security Risk

ABSTRACT

The development of Cross-Border Payments (CBP) offers efficiency while increasing the complexity of risks, particularly those related to data-sharing and data sovereignty in Indonesia. Although previous studies have addressed CBP systems from the perspectives of efficiency, interoperability, and regulation, there is limited research that systematically identifies risks associated with data sharing across jurisdictions. This study identifies and prioritizes key CBP risk factors that directly affect the security of cross-border data sharing and data control. The Fuzzy Delphi Method (FDM) was used to reach expert consensus on the risk factors identified through a systematic literature review. The results indicate that the most critical data-sharing risks in CBP are in the technological and cybersecurity domains, particularly weak data encryption and information transmission problems. The findings confirm that weaknesses in data encryption and transmission security are the primary sources of risk in cross-border data sharing, and have direct implications for data sovereignty. Several factors did not reach the consensus criteria and were not included as key risks in CBP transactions. The main contribution of this study is a consensus-based risk mapping that specifically focuses on the dimensions of data sharing and data sovereignty, along with proposed mitigation strategies grounded in prior research, as recommendations for strengthening the CBP's security architecture and data sovereignty.

This is an open access article under the CC BY-SA license.



Corresponding Author:

Dian Prima Sari,
Faculty of Computer Science,
Universitas Indonesia,
Salembara, Jakarta, Indonesia.
Email: dian.prima32@ui.ac.id

1. INTRODUCTION

CBP is essential to the global financial system, facilitating transactions between payers and payees located in different jurisdictions in various countries [1], [2]. Structurally, CBP systems operate within the framework of an international monetary hierarchy that involves global correspondent banks, central banks, and international financial institutions, forming a pyramid of liabilities that reflects the distribution of global power and liquidity [3]. However, CBP still faces various frictions such as high costs, settlement delays, limited transparency, and limited access, as identified in the G20 Roadmap for Enhancing CBP [4].

According to the 2025 McKinsey Global Payment Report, over the past 30 years, the infrastructure for instant payments has enabled the smooth flow of money across borders [5]. The flow of digital payments is expected to increase in the future, in line with the international commitment, through the Financial Stability Board (FSB), to improve the efficiency of CBP services [6]. The increase in digital payments, especially CBP, is also linked to rising payment fraud globally, and public and private sector stakeholders expressed concern that the payment ecosystem should carefully manage this fraud risk.

By 2026, the G20 has promoted a risk-based approach to CBP, but in reality, 47 jurisdictions (64%) have not conducted comprehensive risk assessments that address operational and governance risks. Information sharing among authorities can support understanding of the risk associated with CBP, as 16 jurisdictions (22%) lack agreement on information sharing or a concrete plan to establish any arrangement in the coming year [4]. The high risk of problems arising from data sharing across jurisdictions has become a fundamental issue in the CBP system. Studies on privacy and security risks in cross-border digital payments emphasize the heightened risk of data breaches, cybercrime, and vulnerabilities in system architecture [7]. In addition, regulations such as the General Data Protection Regulation (GDPR) in Europe and the Personal Data Protection Law in Indonesia add complexity to compliance in cross-border data transfers, especially when data protection standards differ between jurisdictions [8].

CBP systems also serve as instruments of financial statecraft, whereby countries leverage payment infrastructure for strategic and geopolitical purposes [1]. The dominance of certain currencies in the global payment system poses risks to monetary sovereignty and structural dependence for developing countries. Peng [9], states that the fragmentation of cross-border financial policies can increase companies' operational and liquidity risks. FSB, together with the Bank for International Settlement Committee on Payment and Market Infrastructure (BIS-CPMI), has developed a roadmap to improve CBP efficiency, aiming to create transparency and inclusivity while maintaining security and data privacy by 2027 [6].

Although international literature and institutions such as the G20 and BIS have discussed various dimensions of CBP, there remains a research gap in structurally identifying the key risk factors for CBP from the perspectives of institutional experts in developing countries, particularly in Indonesia. Most studies are conceptual, global policy-based, or based on specific regional case studies. However, there has not been much research that systematically identifies and prioritizes risk factors through an institutional expert consensus approach that specifically focuses on the dimensions of data sharing and data sovereignty, as well as proposed mitigation strategies as recommendations for the policy direction in Indonesia, which emphasizes integration, digitization, and strengthening the sovereignty of the payment system [6].

This study seeks to offer a thorough examination of key risk factors for CBP in developing countries by integrating insights from the payment authority, government, and academia. Therefore, this study combines a Systematic Literature Review (SLR) following Kitchenham's protocol and the FDM to establish expert consensus on relevant risk factors in CBP systems and to formulate mitigation strategies grounded in prior research. This research aims to address several research questions, including RQ1. What key risk factors are associated with data sharing in CBP within a developing country? and RQ2. What mitigation strategies are identified in the relevant literature to address these risks?

This study contributes by providing an empirical framework to validate and prioritize CBP key risk factors based on the level of agreement and the intensity of interest among institutional experts. This approach enables the identification of risk factors relevant to the Indonesian payment system. This research is expected to make theoretical contributions to enrich the literature on the identification and prioritization of data-sharing risks in CBP in Indonesia from an institutional expert perspective. The structure of this paper is as follows: Section II presents the research method; Section III describes results and discussion; and Section IV concludes the paper by outlining limitations and suggestions for future research.

2. RESEARCH METHOD

This chapter describes the research methodology employed to determine data-sharing risk factors in CBP in Indonesia. This study relies on an SLR, surveys, and adopts the Fuzzy Delphi approach to systematically analyze CBP risks in Indonesia, as shown in Figure 1.

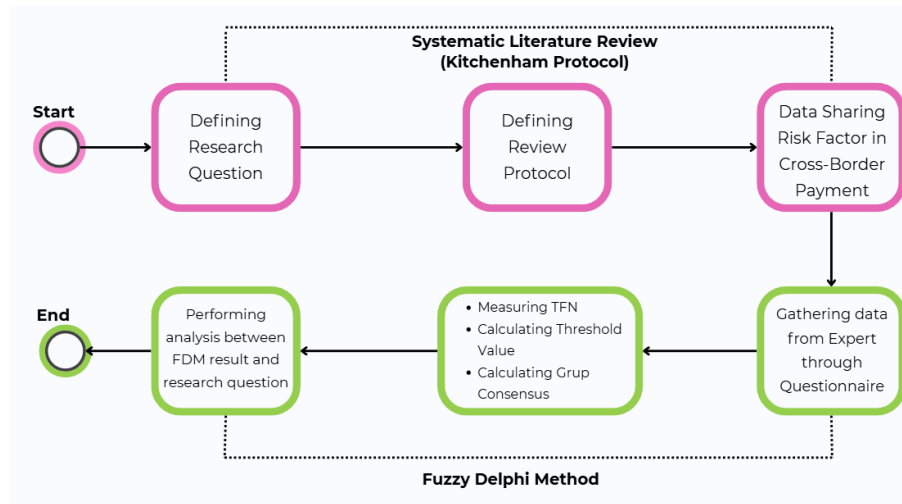


Figure 1. Research Flow

2.1. Systematic Literature Review

This study used an SLR process following the Kitchenham guidelines [10], [11] to review prior studies concerning risk factors in CBP. The Kitchenham method provides a rigorous review methodology for research findings aimed at offering solutions related to software engineering within the required context [10]. The Kitchenham SLR process involves identifying, screening, and analyzing peer-reviewed articles from reputable academic databases. The first step was to address the research questions, RQ1 and RQ2, risk factors, and mitigation strategies. The next step was to identify literature through a comprehensive search of several major academic databases, namely Scopus, IEEE Xplore, ScienceDirect, Taylor & Francis, and ACM Digital Library. Based on the research question, two keyword combinations were applied in the SLR protocol: (1) "Cross-Border" AND "Payment" AND "Information" AND "Security" AND "Risk", (2) "Cross-Border" AND "Payment" AND "Data" AND "Sovereignty" AND "Risk". The initial search identified 2.238 and was narrowed using inclusion and exclusion criteria, as shown in Table 1.

Table 1. Inclusion and Exclusion Criteria

Phases	Inclusion Criteria	Exclusion Criteria
Initiation Phase	- Articles published in English - Articles published from 2021 to 2026 - Peer-reviewed article	- Articles not published in English - Articles not published from 2021 to 2026
Phase 1	- Articles discussing CBP/digital payment - Articles addressing data sovereignty in the CBP context	Duplicate articles
Phase 2	- Open Access - Articles identifying CBP/digital payment/data sovereignty risk factor - Articles employing empirical data analysis	Full-text not available

Table 2 presents the results of the article identification and screening process, starting with the initial stages, Stages 1 and 2

Table 2. Article Identification and Screening Process

Database	Initiation	Phase 1	Phase 2
Scopus	11	4	2
IEEE Xplore	6	4	3
Science Direct	1.144	18	5
Taylor & Francis	343	21	6
ACM Digital Library	734	18	7
Total	2.238	65	23

A total of 23 studies met the criteria and were included in the Quality Assessment Checklist (QAC). The QAC is prepared based on Kitchenham's guidelines [10], that includes the following question:

1. Q1: Is the research objective clearly described?

2. Q2: Is the research methodology appropriate for the problem under consideration?
3. Q3: Do the articles clearly describe issues related to CBP, digital payments, and data sovereignty?
4. Q4: Do the articles present conclusions that are relevant to the research objectives?

According to Kitchenham [10], each question has only three possible answers: “Yes,” “Partially,” or “No”. These three answers are scored as follows: “Yes” = 1, “Partially” = 0.5, and “No” = 0. Consequently, the quality score for a given study is calculated by summing all the response scores for the quality assessment questions. The selected research threshold is 3 to ensure the research can answer most quality questions. Disagreements among authors are resolved through discussion until a consensus is reached. A total of 8 studies received a quality assessment score of 3 or higher and were grouped into 3 domains [12] and the same risk factor will be merged, so the new set of risk factors is presented in Table 1. Details of the articles’ individual scores are presented in Appendix 1. The same risk factor across articles will be merged, and the resulting new group of risk factors is shown in Table 3.

Table 3. Risk Factor of Cross-Border Payment from Literature Review

No	Cross-Border Payment Risk	References
Technological and Cyber Security Risk		
1	Privacy and security breach	[13], [14], [15], [16], [17], [18]
2	Security problems in information transmission	[16], [18], [19], [20]
3	Security problem in payment and settlement	[16], [19], [20]
4	Weak security architecture	[13], [16], [17]
5	Weak data encryption processing ability	[14], [17]
6	Instability in data retrieval from payment systems	[14], [17]
7	Low traceability accuracy	[14]
8	Settlement delay	[16], [17]
Macroeconomic and Regulatory Exposures		
9	Cyber injustice (cybercrime)	[13]
10	Different regulatory regimes across countries	[13], [20]
11	Non-compliance with various policies and regulations	[13], [17], [20]
12	National security risk arising from foreign government access to personal data	[15]
13	Law enforcement due to the foreign government’s access to personal data	[15]
Cultural and Organizational Resistance		
14	Consumers’ attitude towards cashless payment	[13], [17]
15	Inadequate privacy and technology literacy	[13] [23]

2.2. Fuzzy Delphi Method

The screening process for the CBP risk factor was conducted using the FDM. The FDM is a collective decision-making process that involves experts and has been widely used in several cases [21], [22]. While traditional Delphi typically requires multiple rounds, this study adopts the FDM, which allows achieving consensus in a single round by incorporating triangular fuzzy numbers to capture experts’ uncertainty [23], [24]. Additional risk factors suggested by experts in the first round were incorporated into a second round for validation, ensuring their relevance and consensus. According to Rowe and Wright [25], [26], the number of experts recommended by the Delphi panel ranges from 5 to 20, selected for their expertise and contributions to the payment system. According to Jones and Twist [27], the number of expert samples in the Fuzzy Delphi study ranges from 10 to 50 experts to achieve high consistency among experts [24], [27]. Therefore, 10 experts were selected to meet the FDM requirements. A questionnaire was designed to collect expert opinions in this study, with institutional experts in payment systems, information security, and risk management.

The first step is selecting experts, which is crucial for identifying data-sharing risks in CBP. Given their position within the organization, the experts were consulted to collect their feedback on the risk factor relevant to CBP and their level of agreement, ranging from strongly disagree to strongly agree. A 5-point Likert scale was used to express expert opinion, with triangular fuzzy numbers (TFNs) to represent uncertainty. The TFN was defined by three values: minimum (m1), most probable (m2), and maximum (m3), as illustrated in Table 4.

Table 4. Linguistic Scale

5-point Linguistic Scale	FUZZY SCALE		
	M1	M2	M3
5 (strongly agree)	0,6	0,8	1
4 (agree)	0,4	0,6	0,8
3 (neutral)	0,2	0,4	0,6
2 (disagree)	0	0,2	0,4
1 (strongly disagree)	0	0	0,2

An expert chosen as an institutional expert came from the Government, the Payment System Authority, and Academia. Furthermore, the expert should have at least 5 years of experience in payment systems, information systems, or Information Technology (IT) risk management, as detailed in Table 5.

Table 5. Background of Experts

Number of Experts	Specialty	Sector	Current Designation	Years of Experience
E1	Payment System	Payment System Authority	Assistant Director	10 – 15 years
E2	Payment System	Payment System Authority	Deputy Director	10 – 15 years
E3	Payment System	Payment System Authority	Manager	15 – 20 years
E4	Payment System	Payment System Authority	Manager	10 – 15 years
E5	Information Security	Payment System Authority	Information Security Architect	10 – 15 years
E6	IT Risk Management	Payment System Authority	Assistant Director	> 20 years
E7	IT Risk Management	Academic	Lecturer	15 – 20 years
E8	Information Security	Academic	Post Graduate Student	15 – 20 years
E9	Information Security	Government	National Cyber Security Analyst	10 – 15 years
E10	Information Security	Government	National Cyber Security Analyst	5 – 10 years

The second step is filtering, which aims to obtain a final assessment based on TFN. At this stage, the evaluation results are analyzed to determine the relative importance of each criterion and to assess the alternatives being tested. The calculation process involves measuring the distance between the average fuzzy numbers obtained from the experts [28]. The distance between two fuzzy numbers, namely $\tilde{m} = (m1, m2, m3)$ and $\tilde{n} = (n1, n2, n3)$, is calculated using the standardized Euclidean distance formula, namely:

$$d(\tilde{m}, \tilde{n}) = \sqrt{\frac{1}{k} [(m1 - n1)^2 + (m2 - n2)^2 + (m3 - n3)^2]}$$

In the third stage of the FDM procedure, expert consensus testing is carried out by calculating the threshold value, which is represented by d (threshold)[28]. Mathematically, the aggregation is expressed as:

$$\tilde{A} = [\tilde{A}_1, \tilde{A}_2, \dots, \tilde{A}_m] \text{ where } \tilde{A}_i = \tilde{r}_{i1}w_1 + \tilde{r}_{i2}w_2 + \dots + \tilde{r}_{im}w_n$$

Where $\tilde{r}_{in}$ is the triangular fuzzy number value of the n th expert for the i th item, and w_n is the weight given to each expert.

The fourth stage is the stage of determining the final agreement through calculating the group consensus percentage and the defuzzification process[28]. At this stage, each alternative or item is evaluated in the form of a triangular fuzzy number $\tilde{A}_i = (\alpha_{i1}, \alpha_{i3}, \alpha_{i3})$, which is obtained by aggregating the experts' assessments from the previous stage. To convert these fuzzy values into crisp (single) values for ranking and decision-making, a weighted-average defuzzification method is used. Mathematically, the defuzzification value is calculated using the following formula:

$$A_i = \frac{1}{3} (\alpha_{i1} + \alpha_{i2} + \alpha_{i3})$$

This defuzzification process produces a final score for each alternative, which is then used to determine the relative importance level and priority order, and to ensure that the values obtained meet the group consensus acceptance criteria. Thus, this stage serves as a final synthesis process, transforming linguistic uncertainty into quantitative measures that can be analyzed objectively.

3. RESULTS AND DISCUSSION

In evaluating key risk factors for data-sharing risk in CBP, a comprehensive questionnaire for FDM was developed using a linguistic scale. The determination of key risk factors in CBP in Indonesia depends on the fulfillment of three main criteria, namely: (1) A threshold value of less than 0.2, (2) Expert agreement of 75% or more, and (3) A fuzzy score equal to or greater than 0.5 [29], [30]. The defuzzification (dF) process was used to rank the risk factors, and the results for FDM round 1 are presented in Table 6.

In response to RQ1, the results of the calculation of 19 risk factors reveal that 11 risk factors have not met the 3 criteria outlined in the FDM and have not achieved consensus among the expert panel. Four risk factors were rejected, even though they met the threshold of $d < 0.2$ and had an average fuzzy value > 0.5 , but failed to reach expert consensus at 75%. To strictly meet the FDM criteria, these risk factors were rejected.

Table 6. FDM Calculation Round 1

No	Risk Factor	Threshold Value (d) ≤ 0,2	Expert Agreement ≥ 75%	dF Value ≥ 0,5	Ranking	Acceptance
Technological and Cyber Security Risk						
1	Privacy and security breach	0.098	80%	0.760	2	Accepted
2	Security problems in information transmission	0.055	90%	0.780	1	Accepted
3	Security problem in payment and settlement	0,128	70%	0.740	0	Rejected
4	Weak security architecture	0,171	90%	0.720	3	Accepted
5	Weak data encryption processing ability	0,055	90%	0.780	1	Accepted
6	Instability in data retrieval from payment systems	0,196	40%	0.640	0	Rejected
7	Low traceability accuracy	0.153	100%	0.700	4	Accepted
8	Settlement delay	0.214	30%	0.660	0	Rejected
9	Cyber injustice (cybercrime)	0.098	80%	0.760	2	Accepted
Macroeconomic and Regulatory Exposures						
10	Different regulatory regimes across countries	0.257	20%	0.660	0	Rejected
11	Non-compliance with various policies and regulations	0.128	70%	0.740	0	Rejected
12	National security risk arising from foreign government access to personal data	0.153	100%	0.700	4	Accepted
13	Law enforcement due to the foreign government's access to personal data	0.147	100%	0.680	5	Accepted
Cultural and Organizational Resistance						
14	Consumers' attitude towards cashless payment	0.165	50%	0.620	0	Rejected
15	Inadequate privacy and technology literacy	0.147	100%	0.720	3	Accepted

A total of 4 new risk factors were proposed by experts in FDM Round 1, bringing the total to 15 existing and 4 new factors, which were resubmitted in FDM Round 2. The expert panel as a whole chose not to re-evaluate the 15 FDM factors that had already been assessed in Round 1; therefore, the evaluation was conducted only on the 4 additional factors, as shown in Table 7.

Table 7. FDM Calculation Round 2

No	Risk Factor	Threshold Value (d) ≤ 0,2	Expert Agreement ≥ 75%	dF Value ≥ 0,5	Ranking	Acceptance
Technological and Cyber Security Risk						
16	Payment System Provider (PSP) Vulnerability	0.147	100%	0.720	3	Accepted
17	Interoperability Challenges	0.220	40%	0.620	0	Rejected
18	Data integrity and availability Risk	0.153	100%	0.700	4	Accepted
Cultural and Organizational Resistance						
19	Geopolitical Instability	0.244	30%	0.640	0	Rejected

In response to RQ2, mitigation strategies were derived from previous studies, as follows:

3.1 Security problems in information transmission

The transmission of information in digital payments, especially in CBP, can pose significant security issues, particularly for traditional public key encryption algorithms, such as impractical key distribution and management, irrational key distribution, impractical key management and storage, and a high risk of key disclosure [19]. Xiao *et al.* [19] propose a scheme to reduce these risks by establishing a secure payment framework that uses asymmetric encryption and digital signature mechanisms, with particular emphasis on elliptic curve cryptography (ECC). This scheme enhances the reliability and security of information exchange by using two-way authentication between the user's identity and a cryptographic system based on digital signatures. This method not only makes electronic CBP more secure but also makes it run more smoothly, overcoming the security and performance issues common in traditional secure payment systems [19].

3.2 Weak data encryption processing ability

Weaknesses in data encryption processing capabilities in CBP systems can arise when the system's ability to encrypt, store, and retrieve encrypted data is insufficient to handle large transaction volumes securely and efficiently. Ma *et al.* [14] recommend implementing a private-chain blockchain-based architecture with smart contract deployment in Solidity to achieve efficient transaction ciphertext retrieval in blockchain CBP traceability. This method offers the advantages of data encryption processing ability, stable data retrieval, and high traceability accuracy [14]. Alenizi *et al.* [31] also recommend the Integrated Blockchain and Artificial Intelligence (IBAI) framework to improve the security of encrypted data in financial transactions. This approach will ensure the integrity, transparency, and security of the exchange of transaction data [31].

3.3 Privacy and Security Breach

Most previous studies have indicated that privacy and security breaches are risk factors in cross-border payments [13], [14], [15], [16], [17], [18]. Su [16], Ma *et al.* [14], and Chen *et al.* [18] recommend a solution based on blockchain to protect the privacy of individuals and transaction data. Samonte *et al.* [13] recommend strengthening the security architecture based on cryptographic assurance. According to previous research, the use of blockchain is a solution that can reduce the risk of privacy and security breaches in cross-border payments and enhance data protection, transparency, and transaction integrity.

3.4 Cyber injustice (cyber crime)

Cybercrime can pose significant challenges to CBP transactions, particularly in the exchange of financial data and sensitive transaction information across different jurisdictions. Su [16], emphasizes the high risk of fraud and views cybersecurity as a fundamental element (core layer) of cross-border e-commerce systems, not merely an additional feature [16]. Su [16], Zheng [20], and Chen *et al.* [18] recommend a solution based on blockchain to improve cybersecurity in CBP [16], [18]. Meanwhile, Xiao *et al.* [19] recommend security solutions for CBP systems by integrating encryption mechanisms based on digital signatures and asymmetric cryptography. This

will enhance protection against data breaches and unauthorized access in cross-border e-commerce payment systems [19].

3.5 Weak security architecture

Weak security architecture risk in CBP arises when the system infrastructure is not designed with comprehensive protection mechanisms against cyber threats, system failures, and data manipulation. Weak security architecture is characterized by vulnerabilities to data breaches, identity theft, malware attacks, insider abuse, and weak authentication and encryption, leading to fraud and significant financial losses [13]. Samonte *et al.* [13] recommend that mitigating risk requires strengthening the security architecture design to be layered, integrated, and based on cryptographic assurance. In CBP transactions, Su [16] recommends mitigating architectural weaknesses by strengthening a consortium blockchain-based system design with admission control mechanisms, consensus algorithms (e.g., PBFT), and immutable, traceable transaction recording [16]. Another study by Li and Jiang [32] proposes a Secure Hybrid Consensus Protocol (SHCP) architecture to increase security in financial transactions [32].

3.6 Inadequate privacy and technology literacy

The risk of insufficient privacy and technology literacy in CBP systems can arise when consumers lack sufficient understanding of how digital payment technologies work and basic security practices in digital transactions. A comprehensive approach can include strengthening data protection policies and improving public digital literacy through education and training on personal data protection [13]. Therefore, mitigating the risks posed by insufficient privacy and technological literacy in CBP requires not only strengthening the technical architecture but also raising awareness, educating users, and implementing regulations that support inclusion and consumer protection in the digital economy.

3.7 Payment System Provider vulnerabilities

Security provider system vulnerabilities are among the main concerns in digital-based payment and settlement systems, especially for CBP transactions. According to Aljaradat *et al.* [33], mitigation strategies for risk-related cybersecurity for payment systems by leveraging effective incentive programs, investing in security and data protection infrastructure [33]. Law enforcement by payment authority and government in resolving cybercrime cases and implementing stricter penalties for cybercriminals can contribute to increasing clients' trust in digital payment systems [33]. Thus, the weaknesses in the PSP can be addressed by enhancing the security of the PSP's internal systems and through clear regulatory guidelines and law enforcement by policymakers.

3.8 Low traceability accuracy

The risk of low traceability accuracy in CBP systems arises when the system cannot accurately trace the origin of transactions, cash flows, or data links between entities in the payment ecosystem. In the context of CBP, this decline in accuracy can lead to errors in identifying transaction participants, failure to track illegal cash flows, and more complex dispute settlement risks. Similar to the weakness of data encryption, Ma *et al.* [14] suggest that the development of a blockchain-based traceability system with a consensus mechanism, immutable data recording, and integration with personalized recommendations is expected to improve data tracking accuracy. Ahamad *et al.* [34] also suggest Blockchain and Internet of Things (IoT) to improve financial transaction traceability [34].

3.9 National security risk arising from foreign government access to personal data

Security risks related to government access to personal data may arise when transaction and payment data stored by private companies (e.g., cloud providers or PSPs) can be accessed by foreign governments on grounds of national security or law enforcement. As a mitigation measure, a trusted government access framework must be established through a multilateral approach based on the principle of human rights protection and regulate law enforcement agencies' access to data

[15], [35]. Thus, mitigating national security risks in CBP is not only technical but also requires harmonizing international regulations, increasing transparency in government data access, and strengthening rule-of-law and human rights safeguards to maintain a balance between national security and privacy protection in global data flows.

3.10 Data integrity and availability risk

Data integrity and availability risks are critical in CBP e-commerce, particularly because transactions involve the real-time exchange of sensitive data among multiple parties. Xiao *et al.* [19] recommend that the implementation of security mechanisms such as digital signatures, asymmetric encryption, and more effective key management is essential to ensure confidentiality, integrity, and authentication in digital payment processes [19]. Su [16] also proposes blockchain-based mitigation to ensure transaction integrity, immutability, and traceability, as well as to reduce dependence on intermediaries that increase the possibility of attacks [16]. Konatham *et al.* [36] propose an AI-based real-time payment system architecture that integrates microservices, event-driven processing, and cloud-native technologies to enhance scalability and availability. By leveraging Apache Kafka for data streaming, Kubernetes for orchestration, and AI models such as LSTM for fraud detection, the system is capable of processing transactions in real time with low latency and high throughput [36].

3.11 Law enforcement due to foreign government access to personal data

The need for law enforcement agencies to obtain digital evidence poses serious challenges related to data protection, jurisdictional conflicts, and different interpretations of privacy rights [35]. Mitigating these risks requires developing cooperative, human rights-based international legal instruments to regulate law enforcement agencies' access to data [15], [35]. In implementing CBP, mitigating these risks also requires harmonizing data access procedures across countries and clarifying legal dispute-resolution mechanisms so that law enforcement needs do not compromise the principles of personal data protection in CBP systems.

4. CONCLUSION

The findings indicate that the primary risks in implementing CBP are dominated by technical and cybersecurity risks, particularly security problems in information transmission and data encryption process. Additional high-priority risks include privacy breaches, cybercrime, weak security architecture, privacy literacy, PSP vulnerabilities, traceability accuracy, foreign government access to personal data, and data integrity issues. These findings indicate that data protection, information security, and governance of cross-border data access are critical to maintaining security and data sovereignty in the implementation of the CBP in Indonesia. On the other hand, several factors in the technological, regulatory, and cultural domains, including problems in payments and settlement, differences in regulatory regimes, non-compliance with various policies and regulations, and consumer attitudes toward cashless payments, as well as geopolitical instability, did not reach the level of consensus established in this study. This indicates that experts view these factors as not yet being top priorities compared to risks directly related to information security and data protection for CBP implementation in Indonesia.

Overall, the findings provide an empirical basis for developing risk mitigation strategies informed by prior research on data transmission security, encryption capabilities, security architecture, secure cross-border data governance, and data sovereignty protection within CBP implementation. Thus, implementing CBP requires a comprehensive information security approach to safeguard transactions, user trust, and data sovereignty within the cross-border payment ecosystem. This study also has several limitations: the analysis is limited to the CBP system in Indonesia from an institutional expert's perspective, so the characteristics of domestic regulations and CBP infrastructure strongly influence the risk identification results. Further research should consider risk factors identified by experts from the payment system industry to produce a more comprehensive risk identification for the implementation of CBP in Indonesia. Another future research can examine the feasibility of mitigation measures (e.g., costs, implementation constraints, regulatory alignment).

ACKNOWLEDGEMENTS

The authors received no financial support for the research and publication of this article.

CONFLICT OF INTEREST

The authors declare that they have no conflicts of interest regarding the publication of this paper.

DATA AVAILABILITY

The data associated with this study are publicly available online in the replication package. [URL] <https://figshare.com/s/ef0fee24c607012e1804>

AUTHOR CONTRIBUTIONS

Dian Prima Sari: Conceptualization; Data Curation; Formal Analysis; Methodology; Writing-Original Draft. **Yudho Giri Sucahyo:** Supervision.

REFERENCES

- [1] J. Wang, "Financial Statecraft in the Digital Age: FinTech and the Institutional Shifts in China's Cross-Border Payment Sector Since 1993," *J. Contemp. China*, 2025, doi: 10.1080/10670564.2025.2544536.
- [2] E. Cerutti, M. Firat, and M. Hengge, "Global Cross-Border Payments: A \$1 Quadrillion Evolving Market?," 2025.
- [3] A. Arauz, "The International Hierarchy of Money in Cross-Border Payment Systems: Developing Countries' Regulation for Central Bank Digital Currencies and Facebook's Stablecoin," *Int. J. Polit. Econ.*, vol. 50, no. 3, pp. 226–243, 2021, doi: 10.1080/08911916.2021.1984728.
- [4] Financial Stability Board, "G20 Roadmap for Enhancing Cross-border Payments: Consolidated progress report for 2025," FSB, 2025.
- [5] McKinsey, "The 2025 McKinsey Global Payments Report Competing Systems, Contested Outcomes," 2025.
- [6] Bank Indonesia, "Blueprint Sistem Pembayaran Indonesia 2030," Bank Indonesia, 2024.
- [7] N. Allahrakha, G. Xamdarnovna, B. S. Sokhibjonovich, O. Narziev, and P. Temurbek, "Privacy and Security Risks in Cross-Border Digital Payment Systems," *Leg. J. Ilm. Huk.*, vol. 33, no. 2, pp. 553–584, 2025.
- [8] D. S. Guaman, D. Rodriguez, J. M. del Alamo, and J. Such, "Automated GDPR compliance assessment for cross-border personal data transfers in android applications," *Comput. Secur.*, vol. 130, 2023, doi: 10.1016/j.cose.2023.103262.
- [9] X. Peng, "Cross-Border Payments and Corporate Supply Chain Risk: The Heterogeneous Effect of Financial Regulation," *Emerg. Mark. Finance Trade*, 2026, doi: 10.1080/1540496X.2026.2620555.
- [10] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering: A systematic literature review," *Inf. Softw. Technol.*, vol. 51, no. 1, pp. 7–15, 2009, doi: 10.1016/j.infsof.2008.09.009.
- [11] R. Latif, H. Abbas, S. Assar, and Q. Ali, "Cloud computing risk assessment: A systematic literature review," in *Lecture Notes in Electrical Engineering*, 2014, pp. 285–295. doi: 10.1007/978-3-642-40861-8_42.
- [12] C. Betancourt, V. Aranda, C. García, and E. Villanueva, "Strategic Risks and Financial Digitalization: Analyzing the Challenges and Opportunities for Fintech Firms and Neobanks," *J. Risk Financ. Manag.*, vol. 19, no. 1, p. 66, 2026, doi: 10.3390/jrfm19010066.
- [13] M. J. C. Samonte, M. V. O. Ibarreta, K. A. A. Ilagan, and A. R. L. Justo, "Mitigating Risk in the Digital Age: An Analysis of Security Measures for Cashless Payments in Developing Countries," in *2024 4th International Conference on Computer Systems (ICCS)*, 2024, pp. 186–191. doi: 10.1109/ICCS62594.2024.10795842.

- [14] H. Ma, J. Xiao, and Y. Hu, "Research on Security System of Cross-Border Ecommerce Payment under Computer Big Data," in *Proceedings of ICTEI 2023*, 2023, pp. 763–767. doi: 10.1109/ICTEI60496.2023.00137.
- [15] T. Christakis, "Data free flow with trust: current landscape, challenges and opportunities," *J. Cyber Policy*, vol. 9, no. 1, pp. 95–120, 2024, doi: 10.1080/23738871.2024.2421838.
- [16] R. Su, "Enhancing Security and Efficiency in Cross-border E-commerce of Agricultural Products through Intelligent Payment Technology," in *2024 3rd International Conference on Algorithms, Data Mining, and Information Technology (ADMIT)*, 2025, pp. 168–173. doi: 10.1145/3701100.3701136.
- [17] J. Wu, N. Jiang, Z. Wu, and H. Jiang, "Early warning of risks in cross-border mobile payments," *Procedia Comput. Sci.*, vol. 183, pp. 724–732, 2021, doi: 10.1016/j.procs.2021.02.121.
- [18] T.-C. Chen, Y.-S. Liang, P.-S. Ko, and J.-C. Huang, "Optimization Model of Cross-Border E-commerce Payment Security by Blockchain Finance," *Wirel. Commun. Mob. Comput.*, vol. 2021, no. 1, p. 9192219, Jan. 2021, doi: 10.1155/2021/9192219.
- [19] L. Xiao, N. Tuya, and R. Wu, "Application of Computer Database Signature Encryption Algorithm in Cross-Border E-Commerce Payment and Settlement System," in *International Conference on Integrated Intelligence and Communication Systems (ICIICS)*, 2023. doi: 10.1109/ICIICS59993.2023.10421299.
- [20] L. Zheng, "Analysis of Computer-Based Blockchain Technology in Cross-Border E-commerce Platforms," *Mob. Inf. Syst.*, vol. 2022, pp. 1–13, Sep. 2022, doi: 10.1155/2022/5083518.
- [21] B. Lianto, "Identifying Key Assessment Factors for a Company's Innovation Capability Based on Intellectual Capital: An Application of the Fuzzy Delphi Method," *Sustainability*, vol. 15, no. 7, 2023, doi: 10.3390/su15076001.
- [22] A. Rejeb, K. Rejeb, J. G. Keogh, and S. Zailani, "Barriers to Blockchain Adoption in the Circular Economy: A Fuzzy Delphi and Best-Worst Approach," *Sustainability*, vol. 14, no. 6, 2022, doi: 10.3390/su14063611.
- [23] S. H. Hashemi Petrudi, H. Ghomi, and M. Mazaheriasad, "An Integrated Fuzzy Delphi and Best Worst Method (BWM) for performance measurement in higher education," *Decis. Anal. J.*, vol. 4, p. 100121, Sep. 2022, doi: 10.1016/j.dajour.2022.100121.
- [24] A. F. M. Yusoff, A. Hashim, N. Muhamad, and W. N. W. Hamat, "Application of Fuzzy Delphi Technique to Identify the Elements for Designing and Developing the e-PBM PI-Poli Module," *Asian J. Univ. Educ.*, vol. 17, no. 1, pp. 292–304, 2021, doi: 10.24191/ajue.v17i1.12625.
- [25] R. Gene and G. Wright, "Expert opinions in forecasting: The role of the Delphi Technique," 2001, doi: 10.1007/978-0-306-47630-3_7.
- [26] M. Purwaningsih, B. Purwandari, F. P. Sunarso, and F. Setiadi, "Harnessing E-Collaboration for Rural Tourism Recovery after COVID-19: Dual Analysis using SWOT and Porter's Diamond Model," *Emerg. Sci. J.*, vol. 5, no. 4, pp. 559–575, 2021, doi: 10.28991/esj-2021-01297.
- [27] P. M. S. Jones, "Forecasting technology for planning decisions," *Futures*, vol. 11, no. 1, pp. 80–82, 1979, doi: 10.1016/0016-3287(79)90077-6.
- [28] P. Rahayu and I. A. Wulandari, "Defining e-portfolio factor for competency certification using fuzzy delphi method," *Procedia Comput. Sci.*, vol. 197, pp. 566–575, 2021, doi: 10.1016/j.procs.2021.12.174.
- [29] R. Almashhour and A. Alzaatreh, "Identifying building structure factors for urban heat mitigation: a hybrid methodology using Fuzzy Delphi Method and Confirmatory Factor Analysis," *Int. J. Sustain. Energy*, vol. 44, no. 1, 2025, doi: 10.1080/14786451.2025.2457377.
- [30] E. Marlina, A. N. Hidayanto, and B. Purwandari, "Towards a model of research data management readiness in Indonesian context: An investigation of factors and indicators through the fuzzy delphi method," *Libr. Inf. Sci. Res.*, vol. 44, no. 1, 2022, doi: 10.1016/j.lisr.2022.101141.

- [31] A. Alenizi, S. Mishra, and A. Baihan, "Enhancing secure financial transactions through the synergy of blockchain and artificial intelligence," *Ain Shams Eng. J.*, vol. 15, no. 6, p. 102733, Jun. 2024, doi: 10.1016/j.asej.2024.102733.
- [32] S. Li and G. Jiang, "Security and efficiency improvement of internet financial payment based on blockchain technology," *Discov. Comput.*, vol. 28, no. 1, p. 305, Dec. 2025, doi: 10.1007/s10791-025-09835-4.
- [33] A. Aljaradat, G. Sarkar, and S. K. Shukla, "Modelling cybersecurity impacts on digital payment adoption: A game theoretic approach," *J. Econ. Criminol.*, vol. 5, p. 100089, Sep. 2024, doi: 10.1016/j.jeconc.2024.100089.
- [34] S. Ahamad, P. Gupta, P. Bikash Acharjee, K. Padma Kiran, Z. Khan, and M. Faez Hasan, "The role of block chain technology and Internet of Things (IoT) to protect financial transactions in crypto currency market," *Mater. Today Proc.*, vol. 56, pp. 2070–2074, 2022, doi: 10.1016/j.matpr.2021.11.405.
- [35] Master of Science, Criminal Justice, University of New Haven, CT, USA and M. N. I. Khan, "CROSS-BORDER DATA PRIVACY AND LEGAL SUPPORT: A SYSTEMATIC REVIEW OF INTERNATIONAL COMPLIANCE STANDARDS AND CYBER LAW PRACTICES," *Am. J. Sch. Res. Innov.*, vol. 04, no. 01, pp. 138–174, Jan. 2025, doi: 10.63125/a4gbeb22.
- [36] M. R. Konatham, D. P. Uddandaraao, and R. K. Vadlamani, "Engineering Scalable AI Systems for Real-Time Payment Platforms," 2024.
- [37] J. Chu, C. Fang, and K. P. Y. Lai, "Reshaping state-finance-tech nexus through central bank digital currencies: the case of the mBridge project," *Finance Space*, vol. 2, no. 1, pp. 281–304, Dec. 2025, doi: 10.1080/2833115X.2025.2539714.
- [38] J. Buchan and M. Üngör, "Monetary sovereignty in the digital age: the role of Central bank digital currencies," *Int. J. Polit. Econ.*, pp. 1–21, Feb. 2026, doi: 10.1080/08911916.2026.2624900.
- [39] S. Bibi and I. Yerzhan, "Central bank digital currency and digital payment instruments: Kazakhstan's experience between obstacles, threats and opportunities," *J. Post Keynes. Econ.*, vol. 48, no. 3, pp. 575–603, Jul. 2025, doi: 10.1080/01603477.2025.2503149.
- [40] P. Swire, D. Kennedy-Mayo, D. Bagley, S. Krasser, A. Modak, and C. Bausewein, "Risks to cybersecurity from data localization, organized by techniques, tactics and procedures," *J. Cyber Policy*, vol. 9, no. 1, pp. 20–51, Jan. 2024, doi: 10.1080/23738871.2024.2384724.
- [41] Q. Zhu, Y. Ruan, S. Liu, S.-B. Yang, L. Wang, and J. Che, "Cross-border electronic commerce's new path: from literature review to AI text generation," *Data Sci. Manag.*, vol. 6, no. 1, pp. 21–33, Mar. 2023, doi: 10.1016/j.dsm.2022.12.001.
- [42] W. J. K. Almoghayer and H. A. Mahmoud, "The adoption of cross-border payment: A comparative study of belt and road countries," *Borsa Istanbul. Rev.*, vol. 25, no. 6, pp. 1626–1644, Nov. 2025, doi: 10.1016/j.bir.2025.10.011.
- [43] X. Ji, J. Li, and J. Hao, "A Bibliometric Analysis of Risks for Cross-border Business and Data Movement," *Procedia Comput. Sci.*, vol. 242, pp. 1315–1322, 2024, doi: 10.1016/j.procs.2024.08.132.
- [44] O. Bepalova *et al.*, "Crypto assets and CBDCs in Latin America and the Caribbean: Opportunities and risks," *Lat. Am. J. Cent. Bank.*, vol. 6, no. 2, p. 100157, Jun. 2025, doi: 10.1016/j.latchb.2024.100157.
- [45] L. Liu, Q. Chen, Z. Min, C. Shen, and X. Wang, "The impact of cross-border integration of digital products and AIGC in the Metaverse era, Opportunities and Challenges," in *Proceedings of the 2025 11th International Conference on Communication and Information Processing*, Lingshui Hainan China: ACM, Nov. 2025, pp. 592–596. doi: 10.1145/3784833.3784915.
- [46] Y. Liu, F. Lei, and W. Huangcheng, "Design and Implementation of Cross-border E-commerce Risk Control System Based on Machine Learning Algorithm and Computer Simulation," in *Proceedings of the 2024 7th International Conference on Computer Information Science and Artificial Intelligence*, Shaoxing China: ACM, Sep. 2024, pp. 179–184. doi: 10.1145/3703187.3703217.

- [47] J. Ma, X. Jiang, and Y. Yuan, "Challenges and Opportunities of Implementing AI in Cross-Border E-Commerce: A Comparative Study of Industry Practices," in *Proceedings of the 2024 7th International Conference on Information Management and Management Science*, Beijing China: ACM, Aug. 2024, pp. 110–116. doi: 10.1145/3695652.3695701.
- [48] P. Chatzis and E. Stavrou, "Cyber-threat landscape of border control infrastructures," *Int. J. Crit. Infrastruct. Prot.*, vol. 36, p. 100503, Mar. 2022, doi: 10.1016/j.ijcip.2021.100503.
- [49] X. F. Li, Q. Xiang, and H. Cao, "Development Tactics of Cross-border E-commerce under 'One Belt and One Road' Strategy," in *2020 The 4th International Conference on Business and Information Management*, Rome Italy: ACM, Aug. 2020, pp. 106–108. doi: 10.1145/3418653.3418662.
- [50] C.-Y. Liu, T.-Y. Dong, and L.-X. Meng, "Cross-Border Credit Information Sharing Mechanism and Legal Countermeasures Based on Blockchain 3.0," *Mob. Inf. Syst.*, vol. 2022, pp. 1–12, Jul. 2022, doi: 10.1155/2022/6972647.

APPENDIX 1

Appendix 1. The QAC Process

Ref.	Database	Year	Tittle	Score				Total Score
				Q1	Q2	Q3	Q4	
[16]	Scopus	2025	Enhancing Security and Efficiency in Cross-border E-commerce of Agricultural Products through Intelligent Payment Technology	1	1	0.5	1	3.5
[18]	Scopus	2021	Optimization Model of Cross-Border E-commerce Payment Security by Blockchain Finance	1	1	1	1	4
[13]	IEEE Xplore	2024	Mitigating Risk in the Digital Age: An Analysis of Security Measures for Cashless Payments in Developing Countries	1	1	1	1	4
[14]	IEEE Xplore	2023	Research on Security System of Cross-Border Ecommerce Payment under Computer Big Data	1	1	1	1	4
[19]	IEEE Xplore	2023	Application of Computer Database Signature Encryption Algorithm in Cross-Border E-Commerce Payment and Settlement System	1	1	1	1	4
[37]	Taylor & Francis	2025	Reshaping state-finance-tech nexus through central bank digital currencies: the case of the mBridge project	1	1	0.5	0	2.5
[38]	Taylor & Francis	2026	Monetary sovereignty in the digital age: the role of Central bank digital currencies	1	1	0	0	2
[15]	Taylor & Francis	2024	Data free flow with trust: current landscape, challenges and opportunities	1	1	0.5	1	3.5
[39]	Taylor & Francis	2025	Central bank digital currency and digital payment instruments: Kazakhstan's experience between obstacles, threats and opportunities	1	1	0	0	2
[40]	Taylor & Francis	2024	Risks to cybersecurity from data localization, organized by techniques, tactics and procedures	1	1	0	0	2
[1]	Taylor & Francis	2025	Financial Statecraft in the Digital Age: FinTech and the Institutional Shifts in China's Cross-Border Payment Sector Since 1993	1	1	0.5	0	2.5
[41]	Science Direct	2023	Cross-border electronic commerce's new path: from literature review to AI text generation	1	1	0.5	0	2.5
[42]	Science Direct	2025	The adoption of cross-border payment: A comparative study of belt and road countries	1	1	0.5	0	2.5
[17]	Science Direct	2021	Early warning of risks in cross-border mobile payments	1	1	1	1	4
[43]	Science Direct	2024	A Bibliometric Analysis of Risks for Cross-border Business and Data Movement	1	1	0.5	0	2.5
[44]	Science Direct	2025	Crypto assets and CBDCs in Latin America and the Caribbean: Opportunities and risks	1	1	0	0	2
[45]	ACM Digital Library	2026	The impact of cross-border integration of digital products and AIGC in the Metaverse era, Opportunities and Challenges	1	1	0	0	2

Ref.	Database	Year	Title	Score				Total Score
				Q1	Q2	Q3	Q4	
[46]	ACM Digital Library	2024	Design and Implementation of Cross-border E-commerce Risk Control System Based on Machine Learning Algorithm and Computer Simulation	1	1	0.5	0	2.5
[47]	ACM Digital Library	2024	Challenges and Opportunities of Implementing AI in Cross-Border E-Commerce: A Comparative Study of Industry Practices	1	1	0.5	0	2.5
[48]	ACM Digital Library	2022	Cyber-threat landscape of border control infrastructures	1	1	0.5	0	2.5
[20]	ACM Digital Library	2022	Analysis of Computer-Based Blockchain Technology in Cross-Border E-commerce Platforms	1	1	1	0	3
[49]	ACM Digital Library	2020	Development Tactics of Cross-border E-commerce under “One Belt and One Road” Strategy	1	1	0.5	0	2.5
[50]	ACM Digital Library	2022	Cross-Border Credit Information Sharing Mechanism and Legal Countermeasures Based on Blockchain 3.0	1	1	0.5	0	2.5