INTERNATIONAL JOURNAL
ON INFORMATICS VISUALIZATION

journal homepage : www.joiv.org/index.php/joiv

Enhancing Security in Cross-Border Payments: A Cyber Threat Modeling Approach

Amiruddin Amiruddin [a], Obrina Candra Briliyant [b], Susila Windarta [a,*], Muhammad Yusuf Bambang Setiadji [b], Dimas Febriyan Priambodo [a]

[a] *Cybersecurity Engineering, Politeknik Siber dan Sandi Negara, Bogor, Indonesia*
[b] *Cardiff Centre for Cyber Security Research, Cardiff University, Senghennydd Road, Cardiff, England*
*Corresponding author: *susila.windarta@poltekssn.ac.id*

Abstract*—Cross-border payment (CBP) systems are critical to the global economy but are increasingly susceptible to cyber threats due to their complex structures and diverse transaction models. This paper analyzes cyber vulnerabilities across four CBP models: correspondent banking (SWIFT), infrastructure (ApplePay), closed-loop (PayPal), and peer-to-peer (Ripple). It employs the STRIDE methodology and adapts the cyber threat modeling framework proposed by Khalil et al. Key objectives include identifying vulnerabilities, assessing the impact of threats, and proposing mitigation strategies. The corresponding banking model shows the highest threat impact due to extensive transaction elements crossing trust boundaries. In contrast, the closed-loop model demonstrates lower vulnerability because of fewer components outside its trust boundary. Peer-to-peer and infrastructure models present moderate risk levels influenced by blockchain transparency and infrastructure dependencies. Critical threats identified include abuse of authority, malware, and script injection, which can result in significant losses, such as financial theft, service outages, and data breaches. Results indicate that interactions between processes across trust boundaries exacerbate cyber risks. Strategic recommendations include reducing system complexity, reinforcing security protocols at trust boundaries, and integrating advanced threat detection mechanisms. The study highlights these vulnerabilities and risks and underscores the need for robust cybersecurity measures to protect CBP systems. This research contributes to the existing knowledge by providing a detailed threat assessment and practical insights for improving CBP security. Future studies should explore alternative modeling methods, update security contexts to reflect real-world scenarios, and analyze the impact of open banking technologies.

***Keywords*— Cross-border payment; cybersecurity; cyber threats; STRIDE; threat modeling.**

Manuscript received 2 Oct. 2024; revised 19 Apr. 2025; accepted 17 Jun. 2025. Date of publication 30 Nov. 2025.

I. Introduction

Cross-border payment (CBP) facilitates global economic connectivity by allowing payments between financial institutions in different jurisdictions [1]. CBP supports rapid international market expansion and efficient transactions in the digital era, promoting economic growth and easier access to financial services. Technological advancements in CBP reduce transaction costs and currency fluctuation risks, bridging global economic and cultural gaps. Current literature explores various aspects of CBP, including blockchain applications [2], risks associated with emerging technologies [3], and security strategies [4]. Specific studies address interbank CBP security controls like SWIFT [5] and highlight the potential for significant cyber-attacks leading to financial crises [6].

Cyber threat modeling is crucial for identifying and mitigating these risks, and it is discussed through various techniques such as STRIDE, DREAD, and OCTAVE [7]. Khalil et al.'s method [8] for Cyber-Physical Systems (CPS) is adapted for this study. Despite several studies on cyber threats in financial services, there needs to be more detailed evaluations of CBP's security risks [9].

This research applies the STRIDE method to model cyber threats in four CBP models: corresponding bank, closed loop, infrastructure, and peer-to-peer. The STRIDE method is a cybersecurity threat analysis framework developed by Microsoft to identify potential security threats to information systems. STRIDE stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. This method helps identify security threats, increases risk awareness, and enhances system security [10]. This study focuses on specific threats, asset identification, and system architecture based on Bech & Hancock's model [11], acknowledging limitations in the scope and technology considerations. The primary questions are: What are the potential cyber threats to the four CBP models? What factors influence the results of cyber threat modeling in the CBP model?

This work substantially contributes to the existing body of knowledge by conducting a thorough analysis of cyber hazards in Correspondent Banking Payment (CBP) systems using the STRIDE methodology. This research provides significant insights and practical risk management techniques by identifying and analyzing vulnerabilities in various CBP models, such as banking, closed loop, infrastructure, and peer-to-peer platforms. This study focuses on a significant deficiency in the current body of research, providing a thorough analysis of neglected aspects of CBP security. Moreover, it lays a strong groundwork for future studies to improve the security and resilience of CBP systems in the face of ever-changing cyber threats.

A. Cross-Border Payments (CBP)

CBP involves payments between financial institutions in different jurisdictions, facilitating fund transfers across borders and often requiring currency conversion. This system is complex, involving various actors, elements, and processes. The Bank for International Settlements [12] highlights the importance of understanding CBP features to ensure efficient operations. Key features include currency conversion, anti-money laundering (AML) regulations, and Know Your Customer (KYC) protocols, with additional costs such as transaction and intermediary fees. Different CBP models include corresponding banks, closed loops, infrastructure, and peer-to-peer (P2P) systems [11] (see Fig. 1). Each model has unique cost, speed, and availability characteristics, with the corresponding bank model being the earliest and most flexible but also the slowest. Digital technology advancements, including blockchain and digital currencies, are reshaping CBP, making it more efficient and cost-effective [11].

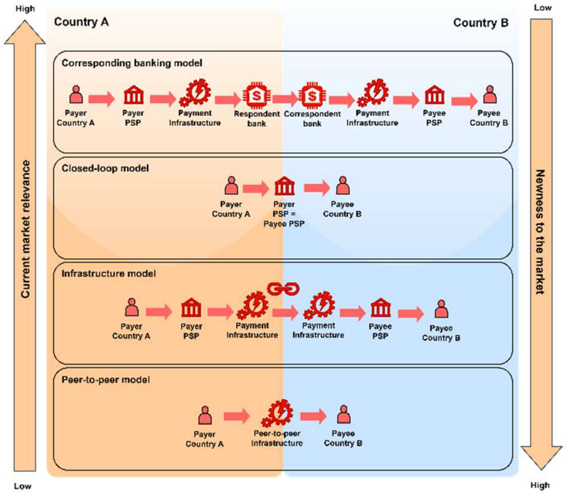


Fig. 1 CBP Models

B. Cyber Threat Modeling

Malicious software (malware) poses significant threats to computer systems, exploiting vulnerabilities and causing severe financial damage, with cybercrime costs reaching more than ten trillion US dollars annually [13]. Effective threat modeling helps identify, assess, and manage potential cybersecurity risks, ensuring digital trust, data protection, legal compliance, and business continuity [14]. Various threat modeling methods, including STRIDE, DREAD, PASTA, and others, provide comprehensive risk assessment frameworks [7], [15]. STRIDE, widely used and integrated into the Microsoft Security Development Cycle, analyzes system components against six security objectives: confidentiality, integrity, availability, authentication, authorization, and non-repudiation [8], [15]. Despite its maturity, no standard procedure exists for applying STRIDE to CBP systems. Research indicates a gap in integrating threat modeling with CBP, necessitating further studies to address this issue [6], [16], [17], [18], [19].

The remainder of this paper is structured as follows: Section 2 reviews the relevant literature, providing a foundation for the study, outlines the research methodology employed in the analysis. Section 4 presents and discusses the findings of the research. Finally, Section 5 offers concluding remarks and suggests directions for future research.

II. Materials and Method

In this study, cyber threat modeling for CBP was conducted using the STRIDE method across four CBP schemes, adapting the framework proposed by Khalil et al. [8]. This adaptation does not include the last two stages (8 and 9), as the research questions have already been answered in stage 7. The adaptation is presented in Fig. 2.

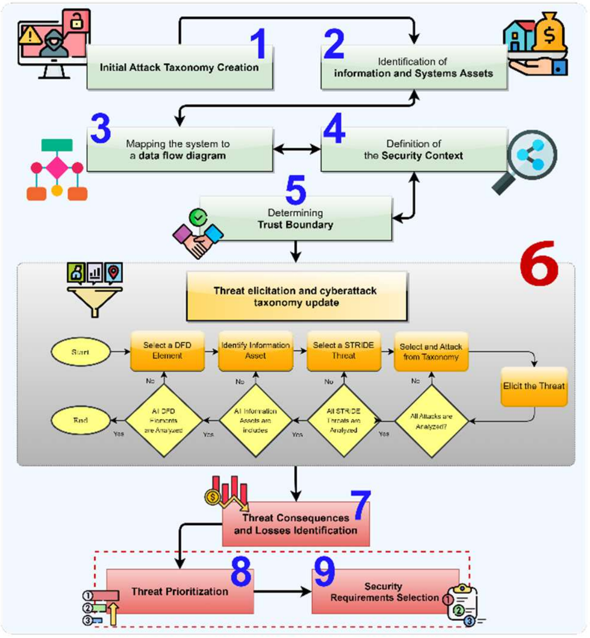

1
Initial Attack Taxonomy Creation
2
Identification of information and Systems Assets
3
Mapping the system to a data flow diagram
4
Definition of the Security Context
5
Determining Trust Boundary
6
Threat elicitation and cyberattack taxonomy update
Start
Select a DFD Element
Identify Information Asset
Select a STRIDE Threat
Select and Attack from Taxonomy
Elicit the Threat
No
No
No
No
All DFD Elements are Analyzed
All Information Assets are includes
All STRIDE Threats are Analyzed
All Attacks are Analyzed?
Yes
Yes
Yes
Yes
End
7
Threat Consequences and Losses Identification
8
Threat Prioritization
9
Security Requirements Selection

Fig. 2 Our research method is adapted from Khalil et al.

A. Cyber Attack Taxonomy Identification:

Cyber-attack taxonomy is a systematic classification of cyber-attacks based on characteristics, methods, and objectives, aiding in developing effective defense strategies. Research highlights that the financial and insurance sector ranks seventh among industries most frequently targeted by cyber-attacks, with diverse attack types driving the need for robust threat modeling [20]. The first stage involved a literature review on cyber-attacks in payment systems, helping us to understand the targeted environment and relevant security issues. This review was focused on CBP attacks, leading to a cyber-attack taxonomy that could be updated during threat elicitation if new attacks were found.

Cyber-attacks on Cross-Border Payment (CBP) systems can be grouped by techniques such as malware, DoS/DDoS, misconfiguration, scams, account takeover, and script injection. Ransomware emerged as the top threat in 2022-2023, accounting for 37.7% of attacks, followed by account takeover at 15%, DoS/DDoS at 2.7%, script injection at 2.05%, and scams and misconfigurations at around 1.5% each (Top 10 cyber-attack techniques 2018-2023) [21].

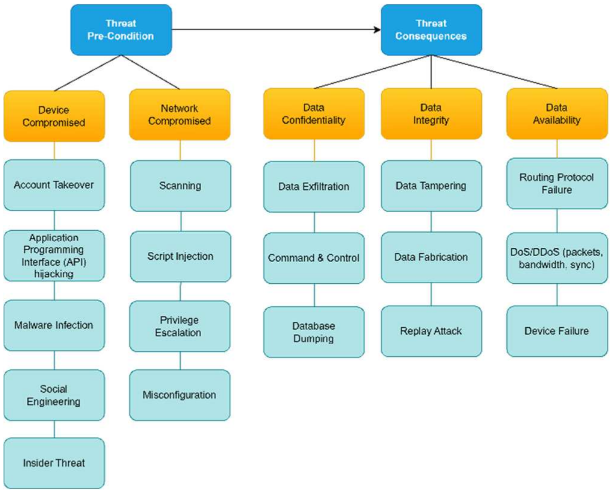


Fig. 3 Cyber-attack taxonomy of CBP

The study identifies that CBP systems face numerous cyber risks in payment systems. While BIS [5] outlines CBP services' functions and features, it does not detail the relevant cyber risks. Simmons et al. [11] developed the AVOIDIT cyber threat taxonomy, classifying attack vectors and their organizational impacts. Fig. 3 displays the consolidated attack taxonomy derived from AVOIDIT, NIST Digital Identity Guidelines, and characteristics from BIS [5]. Fig. 3 is also modified from Khalil et al.'s [9] cyber attack taxonomy with the addition of a confidentiality attack.

B. *Identification of Information Assets and Systems*

This stage aimed to identify and categorize all information assets within the CBP system, with a focus on ensuring the completeness and accuracy of the asset list. Using system architecture diagrams, assets were identified, and potential threats were modeled using the CBP model [11]. We surveyed practitioners and users of CBP services to carry out this identification, and the results are summarized in Table I. In addition to the survey, we reviewed the literature to reinforce the categorization. Ultimately, we determined the focus of the study for threat modeling within the CBP system services. Specifically, we selected SWIFT for the corresponding bank model, PayPal for the Closed-Loop model, ApplePay for the Infrastructure model, and Ripple for the Peer-to-Peer model.

TABLE I
RESULT OF THE QUESTIONNAIRE ON CBP SERVICES/PRODUCTS

Service/ Product	NR	CB	CL	Inf	P2P	Total
Swift	24	24	2	4	3	33
Credit/Debit	12	12	1	19	1	33
Currency Transfer	28	28	0	1	4	33
Remittance	25	25	2	3	3	33
Western Union	7	7	5	17	4	33
Moneygram	10	10	10	10	3	33
Wise	8	8	14	5	6	33
Transfez	11	11	10	7	5	33
Paypal	2	2	21	7	3	33
Alipay	1	1	18	10	4	33
ApplePay	1	1	19	11	2	33
Google Pay	3	3	19	11	0	33
Blockchain	0	0	3	7	23	33

*NR: Number of Respondents, CB: Corresponding Bank, CL: Close Loop, Inf: infrastructure, P2P: Peer-to-peer

1) *Correspondent Bank Model:* The Correspondent bank structure described in BIS publication [22] is depicted in Fig. 4. Notation A indicates that the payer is using a correspondent bank only, and the process begins with number A.5, crediting of bank C account with bank B. Number A.6 payment message from bank B to bank C via a telecommunication network. Number A.7 is the debiting of Bank B's mirror account with Bank C, which is kept for accounting purposes. The last one is number 8, which is crediting the receiver's account with bank C.

Notation B is the involvement of another payment system. The system starts with number B.5, a payment message from bank B to the payment system. Number B.6 is Settlement via the payment system. Number B.7 is a Payment message from the payment system to bank C. The last one, the same as number 8, is crediting the receiver's account with bank C.

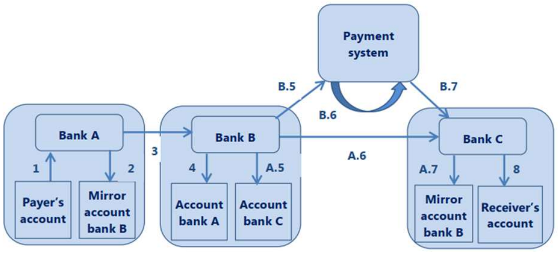


Fig. 4 Correspondent bank payment

2) *Close loop Model:* As the PayPal system in Fig. 5, the closed loop model builds an independent system with microservices based on Node.js. Paypal includes a payment gateway, software that connects a merchant's shopping cart to the processing network. The payment gateway performs security checks to prevent fraud, such as encrypting credit card numbers and verifying digital signatures. Paypal can be connected with a credit card, bank account, debit card information, PayPal balance, and credit from PayPal directly in the PayPal dashboard. From the merchant's point of view, PayPal can be implemented by adding a PayPal icon built with an integrator system from PayPal.

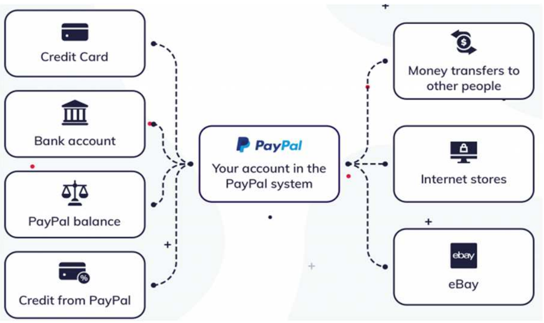


Fig. 5 PayPal payment [23]

3) Infrastructure Model: The infrastructure model uses applications and provides hardware such as identity, point-of-sales tags, etc. Point of Sale (PoS) payment simplifies the payment process by touching a device that stores digital money in a digital wallet. Examples of this technology are ApplePay, SamsungPay, and AndroidPay. Identity in ApplePay adds some biometric security checks by Face Recognition or Face ID and fingerprint or Touch ID, and all of them are secured with a secure enclave, as depicted in Fig. 6. The basis used is the level of penetration and use of ApplePay globally [24], [25].

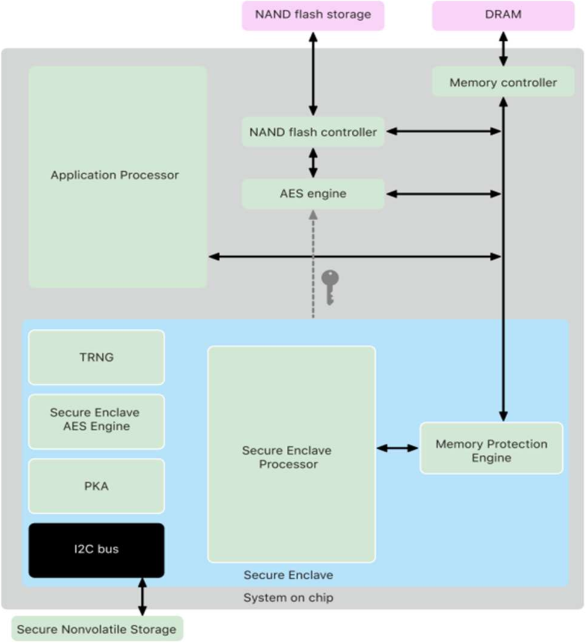


Fig. 6 Secure Enclave [26]

ApplePay payment starts with an iPhone Secure Element (SE) authentication process by adding biometrics (FaceID, Touch ID) or PIN. SE generates a Dynamic Cryptogram consisting of a payment token, amount for payment, or Dynamic CVV using the CVV key by the issuing bank. In general, SE passes the Device Account Number (DAN) using POS specifications related to EMVCo [27].

POS Terminal passes DAN, Dynamic Cryptogram, Dynamic CVV to Acquier bank. In some cases, acquiring banks and merchant banks are different. Merchant banks pass DAN, Dynamic Cryptogram, and Dynamic CVV to the payment network. It passes again to the Token Service Provider (TSP) to generate a Payment Token and look up the real Personal Account Number (AN). Payment Network uses real PAN to contact the issuer bank and the transaction amount, including Transaction Token and Dynamic CVV. CVV decrypted and checked the customer's credit limit or balance in the Issuer bank dynamic. An authorized payment response has been sent back to Payment Network.

4) Peer-to-Peer Model: Ripple is an entity in the financial technology sector that focuses on creating innovations in more efficient cross-border payment solutions. Ripple aims to revolutionize cross-border payment methods by reducing costs, speeding up processes, and increasing transparency in international financial transactions [28]. Central Bank can use Central Bank Digital Currency (CBDC) Private Ledger from Ripple without building a network. Digital Dolar Project [29] works with Ripple in the technical sandbox.

Ripple presents various products and solutions to make cross-border payments more manageable. Core products offered include RippleNet, xCurrent, xRapid, and xVia. xCurrent is a Ripple product that facilitates CBP. According to [30], the Ripple network can handle 1500 transactions per second with a maximum of 5 seconds for settlements and charge approximately $0,0002 for transaction fees.

Payment on Ripple begins with sending institution requests a fiat-to-fiat pricing quote from the receiving institution. Upon receipt, the quote with prenegotiated margins is approved. The sending institution submits payment instructions to the company and debits funds to a digital asset wallet funded by Ripple with XRP. Ripple transfers the funds to the receiver's XRP wallet in 3 to 5 seconds. The receiving institution can immediately pay the end beneficiary in fiat while converting the receiving XRP to fiat currency. The sending institution is invoiced at the start of the following business week after making the payments.

C. *Mapping System to Data Flow Diagram (DFD)*

System architecture diagrams for SWIFT, ApplePay, PayPal, and Ripple were obtained from various sources, mapping entities, processes, interactions, data storage, and data flow into DFDs. Iterations between stages two and three clarified the process.

D. *Security Context Definition and Trust Boundary Determination:*

Determining trust boundaries is based on the security context discussed earlier. Key assumptions significantly impact the chosen trust boundary. For instance, assuming some CBP system components are physically secure without considering the technology provider (vendor neutrality) or excluding wireless connections affects the trust boundary. This is crucial for assessing the trustworthiness of CBP system elements and precisely measuring security risks. Key assumptions influencing trust boundary:

1) Physical Security of CBP Components: Higher trust is placed on data and transaction security if components are assumed to be physically secure. However, this must be tested rigorously as physical attacks remain a threat.

2) Vendor Neutrality: Whether the technology provider necessitates separate trust assessments, adding complexity due to varying security levels.

3) Network security: Assumptions about network safety influence trust in data transmission security. Networks are common weak points in cyber-attacks, requiring careful security consideration.

4) Third-Party Involvement: Trust assumptions about third parties (e.g., cloud service providers) impact data and information security. Contractual clauses on confidentiality, integrity, and data protection are critical in defining trust boundaries in cyber threat modeling.

Transparency in identifying and testing these assumptions in real security contexts is essential. This enables better-informed decisions regarding CBP system security and an understanding of potential risks in a dynamic environment. A significant decision is trusting the organization's internal network while considering potential authority abuse. This includes CBP system components within a single trust boundary of the administering organization (bank/system operator). Consequently, many threats discussed in previous studies (e.g., [31]) are excluded under this assumption.

E. Threat Elicitation and Cyber Attack Taxonomy Update

Focused on producing threat analysis using STRIDE-per-element, each DFD component was individually analyzed. STRIDE-per-interaction, though more complex, was also considered. Deng et al. [32] and Mbaka et al. [33] found STRIDE-per-element to be more comprehensive. This stage highlighted the importance of visibility in threat identification for decision-makers.

F. Threat Consequence and Loss Identification

Conducted by analysts and cybersecurity experts, this stage involves analyzing each potential threat and identifying its impact and potential tangible and intangible losses. The result was a prioritized list of security requirements for enhancing system security, aiding stakeholders in selecting appropriate security controls.

III. Results and Discussion

A. Cyber Attack Taxonomy

Cyber threats are categorized into two groups: threat preconditions and threat consequences. Threat preconditions include device and network compromise, which attackers must access and damage system assets. Threat consequences negatively affect data confidentiality, integrity, and availability. Synchronization between threat preconditions and consequences leads to ultimate threat consequences. For instance, social engineering can compromise devices, impacting all aspects of data security. The implications of the relevant threat to CBP systems are detailed in Table II.

B. Identification of System and Information Asset

Based on the literature study from the 4 CBP models, there are several important assets each. All CBP has four elements: Entity, Process, Data Flows, and Database. Four elements pass the next steps of mapping into DFD.

C. Mapping into DFD and Security Context Analysis

DFD is a visual tool used to describe the system's flow of data and processes. By including cybersecurity aspects in DFD, organizations can identify potential weak points and security risks in data flows.

1) Corresponding Bank Model – SWIFT: The CBP payment chain of the corresponding bank model may also include transfers between institutions within a jurisdiction, which are typically conducted through payment systems. Sometimes, payment systems can also transfer payments through different jurisdictions. DFD of SWIFT can be seen in Fig. 7.

2) Closed Loop Model – PayPal: The closed-loop model does not involve outside parties unrelated to the transaction process. In the context of PayPal, this means that every transaction made through the platform is processed internally by PayPal itself, without involving third parties. The DFD of PayPal is given in Fig. 8.

3) Infrastructure Model – ApplePay: The infrastructure model is another closed loop model with enriching features that connect with the classical banking system. Infrastructure models are also bundled with funding devices and infrastructure. The DFD of the payment process in the infrastructure model is depicted in Fig. 9.

4) Peer-to-Peer Model – Ripple: The peer-to-peer model is a different aspect of the payment system. Classical payment or money must be fully transferred to cryptocurrency. Ripple's xCurrent data flow diagram was created, as shown in Fig. 10.

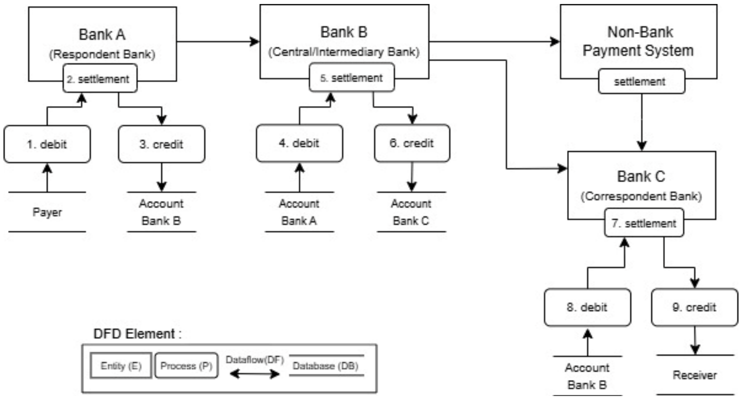


Fig. 7 DFD of SWIFT

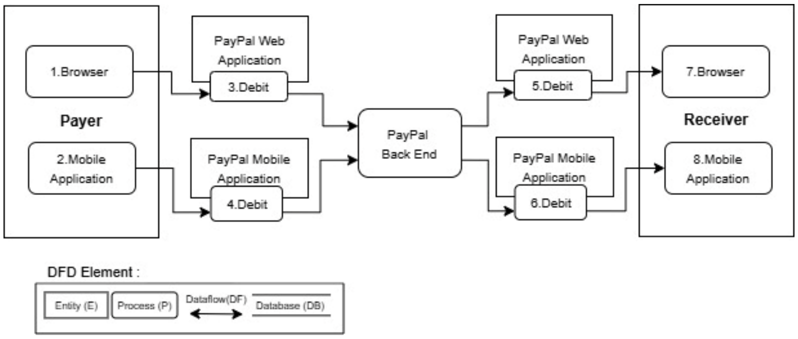


Fig. 8 DFD of PayPal

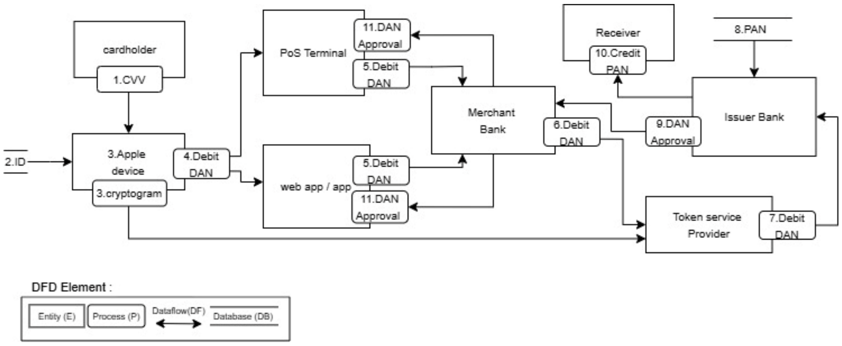


Fig. 9 DFD of ApplePay

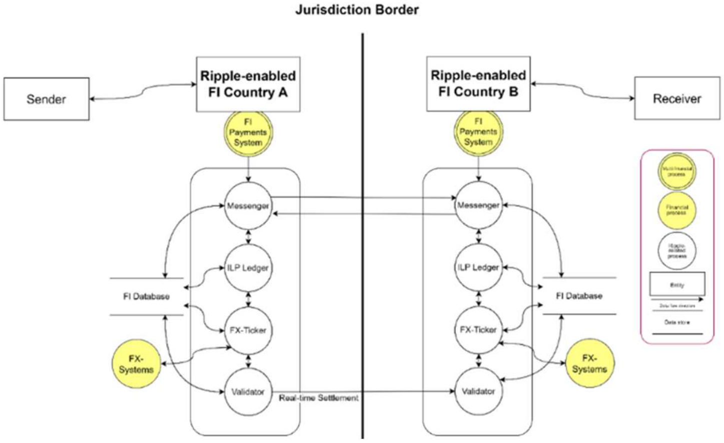
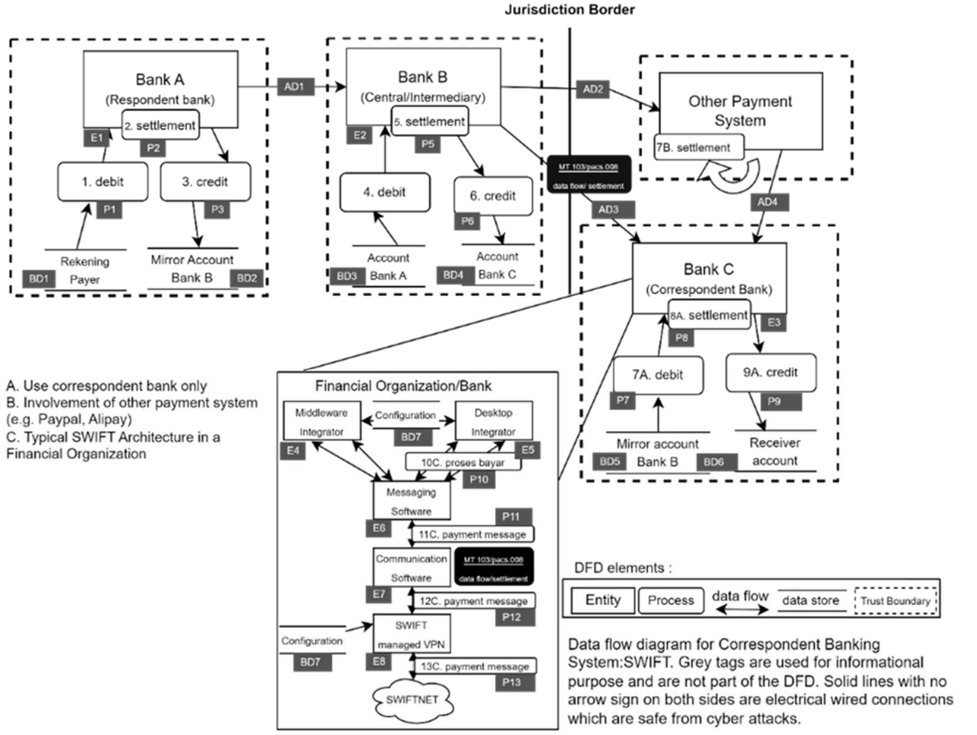


Fig. 10 DFD of Ripple

TABLE II
THREAT CONSEQUENCES (TC)

Threat Code	Threat Precondition	Threat Consequence
TC1	Social engineering, like phishing, business email compromise (BEC)	C, I, A
TC2	Sending malware	C, I, A
TC3	Script Injection	C, I, A
TC4	Misuse of authority (insider threat)	C, I, A
TC5	Attack on API	C, I, A
TC6	Misconfiguration that causes a vulnerability that is easy to exploit	C, I, A
TC7	Privilege escalation	C, I
TC8	Account hijacking/takeover	C, I
TC9	Command & Control (C2)	C, I
TC10	Scanning (port, OS, website)	C
TC11	DoS/DDoS	A
TC12	Message fabrication and modification	I
TC13	Data Exfiltration	C
TC14	Replay attack	I
TC15	Database dumping	C



A. Use correspondent bank only
B. Involvement of other payment system (e.g. Paypal, Alipay)
C. Typical SWIFT Architecture in a Financial Organization

Data flow diagram for Correspondent Banking System:SWIFT. Grey tags are used for informational purpose and are not part of the DFD. Solid lines with no arrow sign on both sides are electrical wired connections which are safe from cyber attacks.

Fig. 11 Cyber threat modeling for SWIFT

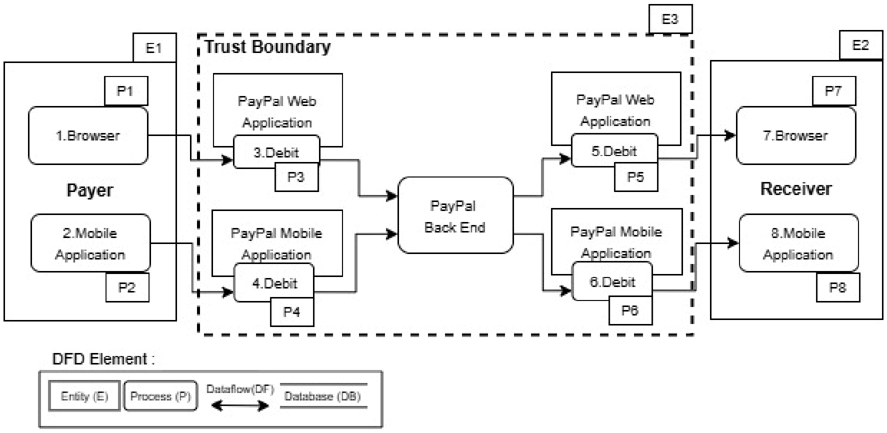


Fig. 12 Cyber threat modeling for PayPal

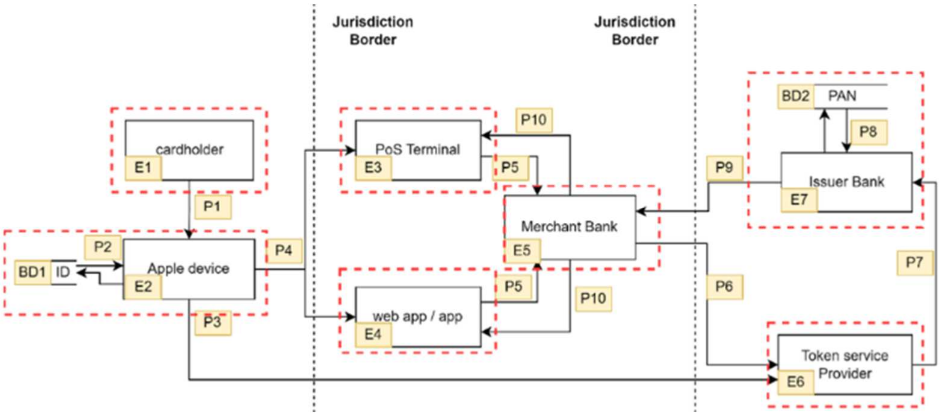


Fig. 13 Cyber threat modeling for ApplePay

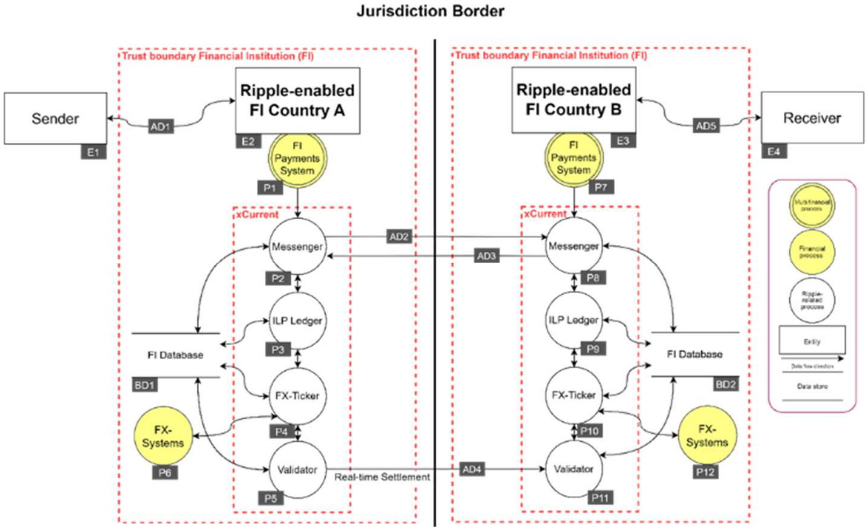


Fig. 14 Cyber threat modeling for Ripple

D. Determination of Trust Boundary

The trust boundary for the corresponding bank is depicted in Fig.11. The Trust Boundary for the closed loop is shown in Fig. 12. The infrastructure model with Apple Pay is shown in Fig. 13. The peer-to-peer model is shown in Fig. 14.

E. Threat Elicitation and Cyber Attack Taxonomy Update

In this stage, each threat definition generated for a particular DFD element has three general components: (1) Threat preconditions derived from the attack taxonomy, (2) Possible attack vectors, and (3) Impacted information assets. To ease the integration between STRIDE and the proposed attack taxonomy, we summarize the STRIDE mapping into the first two components of the proposed threat definition (attack preconditions and possible attack vectors) based on the taxonomy. Table I. Threat Consequences (TC) shows that the Threat Precondition attack state is selected from the attack taxonomy's Device or Network Compromise categories. Processes or databases are assumed to be captured by the Device Compromise category, while Network Compromise attacks information flows. Attack vectors are primarily selected from the attack categories against CIA in the attack taxonomy, except for Spoofing and Escalation of Privilege threats. We assume that attacks can be easily realized once a device or network is compromised. Therefore, we do not add specific attack vectors to the definition of those threat categories; instead, only the keyword "access to" is included in the threat definition.

The threat elicitation stage resulted in 110 threats based on STRIDE, consisting of 12 threats related to spoofing, 23 threats associated with tampering, 17 threats related to denial, 22 threats related to information disclosure, 26 threats about denial of service, and 10 threats related to privilege escalation. We obtained threats related to 7 data flows, 13 processes, 2 data stores, four external entities, and external processes. Trusted data streams are not analyzed at this stage, but they may be interpreted in future threat modeling exercises in case of modification of trust boundaries.

1) Swift:

The SWIFT model's threat modeling is shown in Fig. 11, representing data exchanges within and between financial organizations. Table III details the STRIDE-per-element analysis. Table IV presents the STRIDE-per-interaction analysis.

Table III details the impact of threats on elements in the DFD and their effects on Confidentiality, Integrity, and Availability (CIA). TC1 threats, like social engineering and phishing, affect the CIA across P1-P13. TC3 and TC6 threats, including script injection and misconfiguration, compromise elements E1E8, P2, P5, and P8, affecting integrity and availability. Additionally, TC1 threats can impact accountability (T), hindering the ability to identify and hold perpetrators accountable. Processes and entities in the DFD bank model face spoofing (S) and identity fraud threats from social engineering (TC1), abuse of authority (TC4), and account takeovers (TC8). TC7 and TC8 threats endanger the confidentiality and integrity of DF1, DF3, DB2, and DB5. TC2, TC4, and TC11 threats, such as malware, abuse of authority, and DoS attacks, threaten the availability of DF1-DF4, DB1-DB7, and P1-P13. TC12, involving message fabrication, affects P2, P4, P6, and P8, compromising data integrity.

STRIDE-per-interaction modeling in Table IV shows some interactions are vulnerable to all STRIDE threats, while others are susceptible to specific threats. For instance, interactions between P2-P5 and P5-P8 are vulnerable to all STRIDE elements, while P10-P11 is only vulnerable to S, I, and D. Key messages in the banking model, such as MT103 in the SWIFT system, are crucial for conveying payment orders. MT103 signals are used for fund transfers directly or through intermediary banks between bank accounts. The equivalent ISO 20022 message, pacs.008, transfers customer credit. These messages flow from P2 to P5 (DF1), P5 to P8 (DF3), and P10 to P13, with P2 to P5 being the most critical. Tampering (T) can result from malware (TC2), script injection (TC3), misconfiguration (TC6), and message fabrication (TC12), threatening data integrity and necessitating accurate payment order procedures.

TABLE III
STRIDE-PER-ELEMENT OF SWIFT

STRIDE	DFD Element	Threat Consequence
S	P1-P13, E1-E8	TC1, TC4, TC8
T	DF1-DF4, DB1-DB7, P2, P5, P8	TC2, TC3, TC6, TC12
R	E4-E8, P1, P3, P5, P7, P9	TC5, TC12
I	DF1, DF3, DB2, DB5	TC9, TC13, TC15
D	DF1-DF4, DB1-DB7, P1-P13	TC2, TC4, TC6, TC11
E	P2, P4, P6, P8	TC7, TC10, TC14

TABLE IV
STRIDE-PER-INTERACTION OF SWIFT

Interaction	S	T	R	I	D	E
P2 to P5	√	√	√	√	√	√
P5 to P8	√	√	√	√	√	√
P10 to P11	√			√	√	√
E1 to P3	√	√				
E8 to P13	√	√			√	
DB7 to E4		√			√	
DB7 to E5		√			√	
DB8 to P13		√		√	√	

2) PayPal:

PayPal's threat modeling highlights a shift in attack focus from core systems to user accounts in recent years, emphasizing the importance of user awareness in account protection. Fig. 12 presents PayPal's cyber threat modeling. Tables V and VI show the STRIDE analysis per element and interaction, respectively. Table V reveals that threat TC1, which includes social engineering attacks, phishing, and BEC, impacts confidentiality (C), integrity (I), and availability (A). This demonstrates that phishing attacks threaten the confidentiality, integrity, and availability of processes P1, P2, and entity E1 in the DFD. Similarly, threats TC1 and TC5, such as script injection and parameter fuzzing, can compromise the confidentiality, integrity, and availability of processes P1, P2, and E1. Additionally, threat TC11 impacts the availability of services, threatening data flows DF1 and DF2. Finally, TC2, TC8, and TC12 target entity E1 and process P1 and P2, aiming for unauthorized fund/money transfers.

TABLE V
STRIDE-PER-ELEMENT OF PAYPAL

STRIDE	DFD Element	TC
S	E1, E2, DF1, DF2, DF5, DF6, P1, P2, P7, P8	TC1, TC5, TC8
T	DF1, DF2, DF5, DF6, P1, P2, P7, P8	TC1, TC5
R		
I		
D	DF1, DF2, DF5, DF6	TC11
E	P1, P2, P7, P8	TC2, TC8, TC12

TABLE VI
STRIDE-PER-INTERACTION OF PAYPAL

Interaction	S	T	R	I	D	E
E1 to E3 to E2	√					
P1 to P3	√	√			√	√
P2 to P4	√	√			√	√
P5 to P7	√	√			√	√
P6 to P8	√	√			√	√

3) ApplePay

ApplePay's threat modeling, as illustrated in Fig. 13, emphasizes the boundaries of trust and stakeholder interactions. Several potential threats are identified in the infrastructure model, which is detailed in Table VII. For the Spoofing (S) element, focusing on authenticity, threats such as social engineering (TC1) and malware (TC2) target Entity 1 (E1) to steal sensitive card data. Entity2 (E2) faces threats from malware and account takeovers, indirectly affecting DB1 storage (ID data). Entities E3 to E6, aligned with processes P5 to P7 and P9 to P10, are vulnerable to script injection (TC3) aimed at retrieving sensitive data, though this threat is marked as a void in the model. Despite encryption methods, concerns remain for "store and attack later" methods. Replay attacks (TC14) are excluded due to EMV payment networks, and threats to the database (P8, TC4) are considered in banking threat modeling. For Tampering (T), affecting integrity, DB1 and DB2 face threats from abuse of authority (TC4) and DDoS attacks (TC11). Account takeovers (TC8) and social engineering (TC1) are threats to all processes except P5, which is more focused on API attacks (TC5). Repudiation (R) threats involve social engineering and malware, leading to denial of transactions for E1, and account takeovers (TC8) for E2, which controls ApplePay payments. Information disclosure (I) impacts confidentiality for DB1 and DB2 through insider threats (TC4) and DDoS attacks (TC11). Elevation of privilege (E) threats P1 to P4, allowing unauthorized transactions if sensitive information is obtained. Detailed interactions are provided in Table VIII.

TABLE VII
STRIDE-PER-ELEMENT OF APPLEPAY

STRIDE	DFD Element	TC
S	E1	TC1, TC2
S	E2	TC2, TC8
S	E3-E6	TC3
S	P1, P3, P4	TC1, TC2, TC3, TC8
S	P5, P6, P7, P9, P10	Void
T	P1-P4	TC1, TC8
R	E1	TC1, TC2
R	E2	TC2, TC8
R	E3-E6	TC3
R	P4	TC8
I		
D		
E	P1-P4	TC3, TC8

TABLE VIII
STRIDE-PER-INTERACTION OF APPLEPAY

Interaction	S	T	R	I	D	E
E1 to E2	√		√			
E2 to E6	√		√			
E2 to E3/E4	√		√			
E3/E4 to E5	√		√			
E5 to E6	√		√			
E6 to E7	√		√			
E2 to P3		√				
E3/E4 to P5		√				
P1 to P2	√		√	√	√	
P2 to P3	√	√	√	√	√	√
P3 to P4	√	√	√	√	√	√
P4 to P5	√	√		√	√	

4) Ripple

The threat modeling of Ripple is illustrated in Fig. 14, which provides a comprehensive overview of different relationships and potential threats. The mapping of STRIDE is done for each element in Table IX, based on the threat consequences described in Table I. The Ripple CBP model categorizes different risks to data and systems' confidentiality, integrity, and availability (CIA). Spoofing threats, including identity fraud and social engineering assaults, focus on DFD components E1-E4 by exploiting TC1 risks such as phishing and BEC, which undermine the principles of confidentiality, integrity, and availability (CIA). In addition, TC4 threats, which include the misuse of power, and TC5 threats, which involve API assaults, provide comparable concerns. On the other hand, TC8 threats specifically jeopardize the confidentiality and integrity of data. Tampering threats, which include data manipulation and system integrity disruption, impact the DFD elements P1, P6, P7, and P12 through several threats. These include TC3 threats (script injection), TC6 threats (misconfiguration), TC11 threats (Denial of Service/ Distributed Denial of Service), and TC12 threats (message fabrication/modification). Denial of actions or transactions, known as repudiation threats, influence the elements E1-E4 of the Data Flow Diagram (DFD) through TC1 and TC12 threats, putting at risk the system's confidentiality, integrity, and availability (CIA). Confidential information risks being exposed due to Information Disclosure (I) threats. These threats can influence several elements in the Data Flow Diagram (DFD), namely P1-P12, through TC7 threats (authority escalation), TC9 threats (Command & Control), and TC13 threats (data exfiltration). As a result, the confidentiality and integrity of the information may be compromised. Denial of Service (D) threats cause system unavailability by attacking specific components of the Data Flow Diagram (DFD), namely DF1-DF5. These threats include TC8 (account takeover), TC9 (Command & Control), TC11 (DoS/DDoS), and TC13, which pose risks to both data confidentiality and availability. Elevation of Privilege (E) risks pertain to the manipulation of identity or access privileges, resulting in the compromise of DFD elements P1, P6, P7, and P12 through TC1 (social engineering) and TC12 threats, hence undermining the principles of confidentiality, integrity, and availability (CIA).

The Ripple CBP model utilizes the STRIDE-per-interaction approach to emphasize the intricacy of interactions among processes (P), entities (E), and databases (DB), as shown in Table X. The interactions between entities E1 and E2 and E3 and E4 indicate a possible occurrence of identity fraud. Multiple process interactions, including P1 to P2 and P2 to P3, encompass all STRIDE dangers, emphasizing the necessity for thorough threat mitigation. The hazards associated with STRIDE also apply to process and database interactions, stressing the need to protect data and transactions inside the Ripple CBP network. Furthermore, the presence of various hazards in certain interactions, such as P4 to P6, P10 to P12, P2 to P8, and P8 to P2, highlights the necessity for a holistic approach to mitigate risks. The connection between P5 and P11 presents possible risks of identity and privilege fraud, which require significant attention. Ensuring the integrity and functionality of the Ripple CBP network requires implementing effective security management and mitigation methods. Ripple CBP can establish strong security policies by comprehending these dangers.

F. *Threat Consequences and Loss Identification*

The resulting threat captured at the end of the previous stage (i.e., threat elicitation) includes a definition of the impact on information assets. The threat consequence stage completes elicitation by mapping the threat to potential ultimate losses, including physical impacts. At this stage, we use two terms, Threat Consequence (TC) and Loss (L), to define its implications for people or businesses.

TABLE IX
STRIDE-PER-ELEMENT OF RIPPLE

STRIDE	DFD Element	TC
S	E1-E4, P1-P12	TC1, TC4, TC5, TC8
T	P1, P6, P7, P12, DF1-DF5, DB1, DB2	TC3, TC6, TC11, TC12
R	E1-E4, P1, P6, P7, P12, DB1, DB2	TC1, TC5, TC7
I	P1-P12, DF1-DF5, DB1, DB2	TC7, TC9, TC13
D	DF1-DF5, DB1, DB2	TC8, TC9, TC11, TC13
E	P1, P6, P7, P12	TC1, TC12

TABLE X
STRIDE-PER-INTERACTION OF RIPPLE

Interaction	S	T	R	I	D	E
E1 to E2, E3 to E4	√		√			
P1 to P2, P2 to P3, P3 to P4, P4 to P5, P7 to P8, P8 to P9, P9 to P10, P10 to P11	√	√	√	√	√	√
P2 to DB1, P3 to DB1, P4 to DB1, P5 to DB1, P8 to DB2, P9 to DB2, P10 to DB2, P11 to DB2	√	√		√	√	
P4 to P6, P10 to P12	√	√	√	√	√	√
P2 to P8	√	√	√	√	√	√
P8 to P2	√	√	√	√	√	√
P5 to P11		√			√	√

Threat Consequences briefly describe the immediate consequences of the cyber threat in question, while Costs outline the ultimate costs of the threat. For example, threats against the integrity of CBP system configuration data may make it more susceptible to hacking (i.e., security holes in the operating system), which could result in the loss of funds in the account. We identify potential threat consequences and definitions of harm from the framework proposed by these authors [8], [34], [35].

TABLE XI
DEFINITION AND PRIORITY OF LOSS

Loss Code	Definition of Loss	Priority
L-1	Fund/money loss	Critical (C)
L-2	Payment service stop	High (H)
L-3	Customers' data breach	High (H)
L-4	AML/CFT function and fraud monitoring stop	High (H)
L-5	Settlement function compromised	High (H)
L-6	KYC data management stop	Medium (M)
L-7	Sensitive data breach	Medium (M)
L-8	Profit loss	Medium (M)
L-9	Bad Reputation	Medium (M)
L-10	The currency exchange function is compromised	Medium (M)
L-11	Information loss	Low (L)

In cyber threat modeling, "loss definition and prioritization" refers to defining and prioritizing the various types of losses that can occur due to a cyber attack or cybersecurity incident. The goal is to understand the potential impact and prioritize losses based on their severity. This process helps organizations identify the most significant risks to anticipate losses and allocate security resources and efforts more effectively. The type of loss or impact that may arise from a cyber attack is clearly defined in this process. The loss can cover various aspects such as financial loss, reputation loss, operational loss, data loss, customer trust loss, or even loss of life, especially in critical infrastructure such as energy or health. In the context of this research, these are losses related to the corresponding banking system features, as explained in the BIS Quarterly publication [36]. Once the various types of losses have been defined, the next step is prioritizing or ranking each. This priority can be assigned based on the level of impact, probability of occurrence, or a combination of both. For example, losses with a high impact and high likelihood will receive higher priority than losses with a low impact and a low probability. Table XI contains definitions and priority of losses.

Next, a list of losses that apply to each consequence is mapped out. For example, TC1 (the impact of a social engineering attack) could result in L-1, L-3, L-5, L-7, and L-9 losses. Then, based on the potential loss, a value is given according to the priority level. For example, the cumulative loss of TC1 is considered as 1 Critical (C) + 2 High (H) + 2 Medium (M) + 0 Low (L) to get a weight of 14, as shown in Table XII. Calculating the weight of each TC (WTC) is using equation 1.

$$WTC = C \times 4 + H \times 3 + M \times 2 + L \times 1 \quad (1)$$

C is Critical, H is High, M is medium, L is Low, and 4, 3, 2, and 1 are multiplying factors for C, H, M, and L, respectively. Similarly, we gain a weight of 2 for TC2, 3 for TC3, 1 for TC4, and so on.

G. *Analysis of Modeling Results*

The comparisons of threat modeling results for the four CBP (Cross-Border Payment) models are summarized in Table XIII. The corresponding bank CBP model has the most significant threat impact among the four models, followed by the peer-to-peer, infrastructure, and closed-loop models (see Fig. 15). This ranking correlates with the number of entities, processes, interactions, and interactions between trust boundaries in the CBP architecture. For instance, the closed-loop model has fewer entities, processes, and interactions, especially those outside the trust boundary. This results in fewer cyber threats, mainly limited to abuse of authority and malware introduction due to the social engineering of employees or supply chains.

The peer-to-peer model shares similarities with the closed-loop model but differs in openness. The closed-loop model predominantly uses closed (proprietary) systems with minimally published architecture, while the peer-to-peer model utilizes a blockchain system emphasizing transparency (open source). The types of cyber threats that have the most significant impact on CBP systems are abuse of authority, malware, and script injection, as they directly correlate with the highest potential losses for CBP organizations, such as loss of funds, service disruption, and data leaks. There is a direct correlation between the number of elements (entities, processes, data flows, databases) involved in a single cross-border transaction and the severity of the cyber threat. Each activity in this process has its own threat risk according to the cyber attack stage (reconnaissance, delivery, installation, escalation, exploitation).

When comparing the threats by interaction, the interaction of Process-to-Process outside of the Trust Boundary (PP-Out) has the most significant threat weights, followed by the interaction of Entity-to-Entity outside of the Trust Boundary (EE-Out) as depicted in Fig. 16. Additionally, it was found that interactions involving processes—both processes to other processes and processes to different elements (entities, databases)—have the greatest threat consequences in all CBP models, resulting in a high cyber threat weight. Therefore, the more processes involved in cross-border transactions, the higher the impact (weight) of the potential threat on CBP's business. Processes occurring at different trust boundaries (e.g., across organizations or work units) significantly influence the increasing consequences of losses or cyber threats' impact (weight).

TABLE XII
THREAT CONSEQUENCES (TC) WEIGHT AND RANK

TC	Type	Loss	C	H	M	L	Weight	Rank
TC1	Social engineering	L-1, L-5, L-3, L-7, L-9	1	2	2	0	14	8
TC2	Malware	L-1, L-2, L-3, L-4, L-5, L-7, L-10	1	4	2	0	20	2
TC3	Script injection	L-2, L-3, L-4, L-5, L-6, L-7, L-11	0	5	1	1	18	3
TC4	Abuse of authority	L-1, L-2, L-3, L-4, L-5, L-7, L-9, L-10	1	4	3	0	22	1
TC5	Attack on API	L-2, L-4, L-5, L-6, L-7, L-10	0	3	3	0	15	6
TC6	Misconfiguration	L-2, L-3, L-4, L-5, L-6, L-7, L-11	0	4	2	1	17	4
TC7	Privilege escalation	L-3, L-5, L-7, L-8, L-10	0	2	3	0	12	10
TC8	Account hijacking/takeover	L-1, L-2, L-5, L-3, L-7, L-9	1	3	2	0	17	4
TC9	Command & Control (C2)	L-3, L-5, L-7, L-10, L-11	0	2	2	1	11	11
TC10	Scanning	L-2, L-4, L-5, L-6, L-7, L-11	0	3	2	1	14	8
TC11	DoS/DDoS	L-2, L-4, L-5, L-6, L-8, L-9	0	3	3	0	15	6
TC12	Message fabrication or modification	L-1, L-5, L-9, L-10	1	1	2	0	11	11
TC13	Data exfiltration	L-3, L-7, L-9, L-11	0	1	2	1	8	13
TC14	Replay attack	L-5, L-7, L-10	0	1	2	0	7	14
TC15	Database dumping	L-3, L-7, L-9	0	1	2	0	7	14

TABLE XIII
INTERACTION WEIGHTS AND STRIDE THREATS FOR ALL CBP MODELS

Code	Type	Trust Boundary	Corresponding Bank	W	Closed-Loop	W	Infrastructure	W	Peer-to-Peer	W	STRIDE
PP-out	Process-Process	Outside	P2->P5, P5->P8	66	P1->P3, P2->P4, P5->P7, P6->P8	77	P1->P2, P2->P3, P3->P4, P4->P5	69	P2->P8, P8->P2, P5->P11	40	S, T, R, I, D, E
PP-in	Process-Process	Inside	P10->P11	29	N/A	0	N/A	0	P1->P2, P2->P3, P3->P4, P4->P5, P7->P8, P8->P9, P9->P10, P10->P11	49	S, I, D
EP-out	Entity-Process	Outside	N/A	0	N/A	0	E2->P2, E3/E4->P5	15	N/A	0	S, T
EP-in	Entity-Process	Inside	E1->P3, E8->P14	48	N/A	0	N/A	0	N/A	0	S, T, D
DE-out	Database-Entity	Outside	N/A	0	N/A	0	N/A	0	N/A	0	-
DE-in	Database-Entity	Inside	E4->DB7, E5->DB7	37	N/A	0	N/A	0	N/A	0	T, I, D
DP-out	Database-Process	Outside	N/A	0	N/A	0	N/A	0	N/A	0	T, D
DP-in	Database-Process	Inside	P13->DB7	39	N/A	0	N/A	0	P2->DB1, P3->DB1, P4->DB1, P5->DB1, P8->DB2, P9->DB2, P10->DB2, P11->DB2	24	T, I, D
EE-out	Entity-Entity	Outside	N/A	0	E1->E3, E3->E2	46	E1->E2, E2->E6, E2->E3/E4, E3/E4->E5, E5->E6, E6->E7	69	E1->E2, E3->E4	80	S, R
EE-in	Entity-Entity	Inside	N/A	0	N/A	0	N/A	0	N/A	0	-
Total				219		123		153		193	

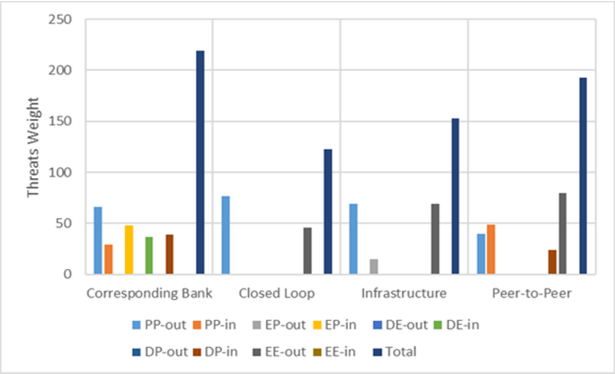


Fig. 15 Threats weight per CBP model

This research assumes the organization's internal network is trusted or within the same trust boundary. Within the same trust boundary, the possibility of cyber threats such as misuse of authority, insider threats, or social engineering (as seen in the Stuxnet incident) is still considered. This assumption implies that the components of the CBP system are within the same trust boundary within a single CBP administering organization (i.e., a bank or system operator). Quantitatively, it was found that more cyber threats occur within the limits of trust (internal organizations/work units/groups), while qualitatively (threat weight), the most significant threat impact is the interaction of elements between organizations/work units/groups. The types of cyber threats with the greatest impact on CBP systems are abuse of authority, malware, and script injection, as they directly correlate with the highest potential losses for the CBP organization, such as loss of funds, service disruption, and data leaks.

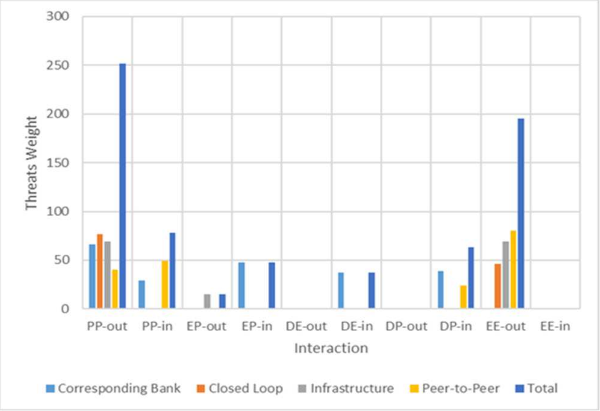


Fig. 16 Threat weights per interaction

H. Security Control Recommendation and Standards/Best Practices

Based on the potential threats identified from previous threat modeling of the four CBP (Cross-Border Payment) models, security controls are recommended according to standards or best practices for each potential threat category and the corresponding cyber kill chain stages. Table XIV provides a detailed overview of these recommendations. For example, in Process-Process transactions outside the Trust Circle (coded as PP-Out), threats include malware, script injection, misconfiguration, and data fabrication or modification.

TABLE XIV
SECURITY CONTROL RECOMMENDATION BASED ON CYBER KILL CHAIN STAGES

Code	Threats	Reconnaissance	Delivery	Installation	Connect to CC	Exploitation
PP-out	Malware, Script injection, Misconfiguration, Data fabrication or modification	Close/turn off unneeded ports, services, apps, and servers (hardening); network segmentation; public IP information anonymization; apply Transport Control Protocol (TCP) Wrapper.	E-mail link filtering and scanning (DKIM, DMARC, SPF); disable macro functions in document files and autorun in OS; implement an intrusion prevention system (IPS), implement Security Incident and Event Management (SIEM); Implement centralized security features on user devices including personal devices (e.g. Host IPS, mobile device management), Use application whitelists; blocks the use of USB drives on the core system (physical, logical or both).	Implementing file integrity monitoring mechanisms; implementing a separation of duties policy; supervising and limiting administrator privileges	Log recording and monitoring (e.g., daily transaction of SWIFT, user/admin log)	Use encryption (website, database, intranet/supply chain); apply Data Leakage Prevention (DLP)
PP-in	Social engineering, Malware, and API attacks	Implement strong password policies and technology and add access controls (e.g., two-factor authentication).	Implement API security policies and technology (tokens, authentication, secure coding, web API); use VPN for remote workers.	Differentiate privileges between users and admins. Only admins can install applications.	Filter data that will come out of the trust boundary	Implement Know Your Customer (KYC) procedures to ensure that customers and businesses involved in transactions have valid identities
EP-out	Distributed Denial of Services (DDoS)	Use third-party services for IP address masking (Akamai, Cloudflare); configure DNS properly, correctly, and securely so that it does not reveal the IP address.	Implement an intrusion prevention system (IPS); implement Security Incident and Event Management (SIEM); Use third-party services for load balancer (Akamai, Cloudflare)	N/A	N/A	Implement data backup (backup system)
EP-in	Account takeover, Authority Escalation, Command and Control (C2), Data exfiltration	Apply updates to the OS, applications, and devices used (patching & updating).	Implement file integrity monitoring.	Ensure the implementation of Secure Software Development in application/system procurement; carry out penetration tests on applications/systems before use.	Implement network access controls (best using electronic certificates) on all devices, especially those that can access critical systems; implement DNS redirects and DNS sinkholes to make C2	Implement Data Leakage Prevention (DLP)

Code	Threats	Reconnaissance	Delivery	Installation	Connect to CC	Exploitation
					communications more difficult.	
DE-out	N/A	N/A	N/A	N/A	N/A	N/A
DE-in	Disrupting services with DoS/DDoS, abuse of authority, database dumping	Perform network traffic filtering using a firewall/proxy/router; block the use of USB drives on the core system (physical, logical, or both)	Implement a policy of separation of duties, minimum authority (least privilege), and job rotation	N/A	N/A	Implement data backup (backup system); Implement encryption (web, database, internal network/supply chain); implement Data Leakage Prevention (DLP)
DP-out	N/A	N/A	N/A	N/A	N/A	N/A
DP-in	Disrupting services by DoS/DDoS, Data fabrication/modification, Abuse of authority	Use vulnerability assessment and take subsequent action to close any gaps found in the scan.	Implement file integrity monitoring.	Implement a policy of separation of duties, minimum authority (least privilege), and job rotation.	N/A	N/A
EE-out	Sending malware, Script injection, Account takeover, Data fabrication/modification	Run an information security awareness program; Update the OS, applications, and devices (patching and updating).	Implement an Access Control List (ACL) and demilitarized zone (DMZ) in the network.	Implement threat hunting; Implement anti-bot, anti-virus, or anti-malware	Implement internal network anomaly detection capabilities; Implement DNS redirection and DNS sinkhole	N/A
EE-in	N/A	N/A	N/A	N/A	N/A	N/A

Recommendations to mitigate these threats during the installation stage include closing or turning off unnecessary ports, services, applications, and servers (hardening), implementing network segmentation, anonymizing public IP information, and applying Transport Control Protocol (TCP) Wrappers. For the exploitation stage, it is recommended to use encryption for websites, databases, and intranets/supply chains, and to apply Data Leakage Prevention measures. These recommendations align with the standards and best practices in Table XV.

TABLE XV
SECURITY CONTROL RECOMMENDATION CONFORMITY WITH STANDARDS/BEST PRACTICES

No.	Required for threat mitigation	Standards/Best Practices
1	Guidance on protecting against malware	ISO/IEC 27001:2022 [37], NIST Cybersecurity Framework, and CIS Controls
2	Guidance on securing applications	OWASP for Application Security Verification Standard, PCI DSS, and ISO/IEC 27001:2022
3	Guidelines for Secure Configuration Practices	CIS Controls, ISO/IEC 27001:2022, and NIST SP 800-53
4	Guidance on data integrity controls	ISO/IEC 27002 and NIST SP 800-53
5	Controls related to social engineering and user awareness	NIST SP 800-53, ISO/IEC 27001:2022, and GDPR
6	Guidance on securing APIs	OWASP API Security, ISO/IEC 27001:2022, and NIST SP 800-53
7	Guidelines for digital identity and authentication	OWASP and the Cloud Security Alliance (CSA) for DDoS attack, NIST Special Publication 800-63A-4 [38]
8	Framework for information security management	ISO/IEC 27001:2022
9	Continuous monitoring for unusual network traffic	CIS Controls and NIST Cybersecurity Framework
10	Guidance on protecting sensitive data	GDPR, PCI DSS, and ISO/IEC 27002
11	Guidance on mitigating DoS/DDoS attacks	OWASP, CSA, and the National Institute of Standards and Technology (NIST)
12	Controls for managing user access	ISO/IEC 27001:2022 and NIST SP 800-53
13	Guidance on securing databases	ISO/IEC 27002 and OWASP

Similarly, there are no security control recommendations in Database-Entity transactions inside the Trust Boundary (coded as DE-In) for the Reconnaissance and C&C Connection stages. DE-In transactions are specific to the Corresponding Bank model, where threats include tampering, information disclosure, and denial-of-service (DoS) attacks. Technical threats for these scenarios could involve disrupting services with DoS/DDoS, abuse of authority, and database dumping. Thus, for the Reconnaissance stage, the recommendation is to utilize third-party services to conceal IP addresses (such as Akamai or CloudFlare) and properly configure DNS to prevent IP address disclosure. For the C&C Connection stage, recommendations include controlling network access for computers and devices, especially those accessing critical systems; implementing DNS redirection and DNS sinkholes to complicate C&C communications; and encrypting sensitive data.

Based on this discussion, CBP organizations must delve deeply into the cyberattack chain targeting CBP systems and implement layered security controls using a defense-in-depth approach. Businesses must provide comprehensive support to IT and information security teams to establish and maintain a robust security posture around CBP infrastructure, considered the organization's primary asset or "crown jewel." Securing an organization's CBP infrastructure is a business responsibility facilitated by IT and information security functions. Financial organizations must recognize the cyber threats to their payment system infrastructure and take proactive measures to mitigate the impact of potential attacks.

IV. Conclusion

This study modeled threats on four CBP models to identify potential risks and propose mitigations. The findings suggest that the closed-loop model has fewer DFD elements outside the trust boundary, indicating a lower susceptibility to cyber threats than other models. The main risks in the closed-loop model are the misuse of power and the introduction of malware through social engineering or supply chains. Similarly, the peer-to-peer model has minimal components beyond the trust boundary but utilizes transparent blockchain technology. Using the STRIDE technique, the corresponding bank CBP model exhibited the most significant threat impact, followed by the peer-to-peer, infrastructure, and closed-loop models. This is attributed to the numerous elements involved in each transaction, each with potential risks at various stages of a cyber-attack. Cyber risks are particularly heightened by interactions that cross organizational and trust boundaries. While the study assumes the reliability of internal networks, it also considers insider threats, indicating that the most substantial impact arises when different organizational elements interact.

Strategic recommendations include streamlining CBP models by reducing entities, processes, and interactions; minimizing interactions between trust boundaries and implementing multiple security layers; addressing critical vulnerabilities such as misuse of power, malware, and unauthorized code insertion in security protocols; and using well-tested, reliable technologies balancing proprietary and open-source options.

Future research must address emerging paradigms in cross-border payment (CBP) security, such as open banking APIs, Central Bank Digital Currencies (CBDCs), embedded finance platforms, and the rising use of artificial intelligence (AI) and machine learning (ML). These innovations create new trust boundaries, third-party integrations, and authentication layers, so threat modeling needs to evolve beyond STRIDE toward attack trees and ML-driven classification. AI promises stronger fraud-detection models, real-time behavioral analytics, and predictive exchange-rate forecasting, elevating the security baseline; yet it also introduces unresolved challenges—privacy-preserving model training, algorithmic bias in high-risk decisions, and dependence on resilient AI components capable of withstanding adversarial manipulation. Future work should therefore deliver benchmarking datasets, fairness metrics, privacy-enhancing techniques such as federated learning and differential privacy, along with tailored security controls for dynamic consent management and continuous fraud detection within these rapidly changing ecosystems.

Limitations

This study provides a structured and comprehensive STRIDE-based threat modeling approach for CBP systems but does not incorporate real-time operational data or red-teaming simulations. The assumption of internal network trust could underestimate insider threats in highly federated or multi-stakeholder ecosystems. Also, the exclusion of multi-party interaction validation and adversarial testing limits its predictive capabilities under evolving threat conditions. These constraints should be addressed in follow-up research through the inclusion of synthetic attack data, live incident mapping, and multi-sectoral expert reviews.

Acknowledgment

We sincerely thank Bank Indonesia for their invaluable support through the Research Grant Bank Indonesia (RGBI), Number 25/18/PKS/BINS/2023. This study would not have been possible without their generous financial assistance. We sincerely appreciate their commitment to fostering research and innovation.

References

[1] Committee on Payments and Market Infrastructures, "Cross-border retail payments," Bank for International Settlements, Basel, Switzerland, Rep. d173, 2018. Accessed: Jun. 02, 2025. [Online]. Available: https://www.bis.org/cpmi/publ/d173.pdf.

[2] Q. Liao and M. Shao, "Discussion on payment application in cross-border e-commerce platform from the perspective of blockchain," in *E3S Web Conf.*, vol. 235, p. 03020, 2021, doi:10.1051/e3sconf/202123503020.

[3] Q. Liao and Y. Wang, "Prospect and challenges of cross-border payment posed by digital currency - From the perspective of blockchain coalition," in *E3S Web Conf.*, vol. 218, p. 04001, Dec. 2020, doi: 10.1051/e3sconf/202021804001.

[4] W. Lei, "Study on security countermeasures of cross-border e-commerce payment risk," *J. Phys. Conf. Ser.*, vol. 1616, no. 1, p. 012042, 2020, doi: 10.1088/1742-6596/1616/1/012042.

[5] A. D. Zisopoulos, K. G. Panitsidis, G. K. Broni, and N. D. Kartalis, "Cross border interbank payment system (CIPS) security supplements; tangible radio safety box, software as non-textual password and revolving executable code modules," *WSEAS Trans. Bus. Econ.*, vol. 20, pp. 273–283, 2023, doi: 10.37394/23207.2023.20.26.

[6] K. Huang and S. Madnick, "Cyber securing cross-border financial services: The need for a financial cybersecurity action task force," *J. Inf. Syst. Secur.*, vol. 16, no. 2, pp. 79–97, 2020, doi:10.2139/ssrn.3544325.

[7] A. Konev *et al.*, "A survey on threat-modeling techniques: Protected objects and classification of threats," *Symmetry*, vol. 14, no. 3, p. 549, 2022, doi: 10.3390/sym14030549.

[8] S. M. Khalil *et al.*, "Threat modeling of cyber-physical systems - A case study of a microgrid system," *Comput. Secur.*, vol. 124, p. 102950, 2022, doi: 10.1016/j.cose.2022.102950.

[9] W. Xiong and R. Lagerström, "Threat modeling - A systematic literature review," *Comput. Secur.*, vol. 84, pp. 53–69, 2019, doi:10.1016/j.cose.2019.03.010.

[10] P. Das *et al.*, "STRIDE-based cybersecurity threat modeling, risk assessment and treatment of an in-vehicle infotainment system," *Vehicles*, vol. 6, no. 3, pp. 1140–1163, Jun. 2024, doi:10.3390/vehicles6030054.

[11] M. Bech and J. Hancock, "Innovations in payments," *BIS Quart. Rev.*, pp. 21–36, Mar. 2020. Accessed: Mar. 15, 2023. [Online]. Available: https://www.bis.org/publ/qtrpdf/r_qt2003f.pdf.

[12] Bank for International Settlements, "Annual economic report 2020," Bank for International Settlements, Basel, Switzerland, 2020. Accessed: Oct. 05, 2025. [Online]. Available: https://www.bis.org/publ/arpdf/ar2020e.pdf.

[13] E. V. Cobos, S. Cakir, S. Straub, C. Z. Qiang, and C. Torgusson, "A review of the economic costs of cyber incidents," World Bank, Washington, DC, USA, Rep. 193919, 2024.

[14] World Economic Forum, "Earning digital trust: Decision-making for trustworthy technologies," World Economic Forum, Cologny, Switzerland, 2022. [Online]. Available: https://www3.weforum.org/docs/WEF_Earning_Digital_Trust_2022.pdf.

[15] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "STRIDE-based threat modeling for cyber-physical systems," in *2017 IEEE PES Innov. Smart Grid Technol. Conf. Europe (ISGT-Europe)*, Sep. 2017, pp. 1–6, doi: 10.1109/ISGTEurope.2017.8260283.

[16] A. Zhou, G. Su, S. Zhu, and H. Ma, "Invisible QR code hijacking using smart LED," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 3, no. 3, pp. 1–23, Sep. 2019, doi: 10.1145/3351284.

[17] N. AllahRakha, T. G. Xamdamovna, B. S. Sokhibjonovich, O. Narziev, and P. Temurbek, "Privacy and security risks in cross-border digital payment systems," *Legality J. Ilmiah Hukum*, vol. 33, no. 2, pp. 553–584, Sep. 2025, doi: 10.22219/ljih.v33i2.40400.

[18] Y. Ting, Y. Azura, M. A. Azad, and Y. Ahmed, "An integrated cyber security risk management framework for online banking systems," *J. Bank. Financ. Technol.*, pp. 1–20, May 2025, doi: 10.1007/s42786-025-00056-3.

[19] Y. Y. Nizovtsev, O. A. Parfylo, O. O. Barabash, S. G. Kyrenko, and N. V. Smetanina, "Mechanisms of money laundering obtained from cybercrime: The legal aspect," *J. Money Laund. Control*, vol. 25, no. 2, pp. 297–305, Apr. 2022, doi: 10.1108/JMLC-02-2021-0015.

[20] A. A. Darem *et al.*, "Cyber threats classifications and countermeasures in banking and financial sector," *IEEE Access*, vol. 11, pp. 125138–125158, 2023, doi: 10.1109/access.2023.3327016.

[21] Hackmageddon, "Cyber attacks statistics," 2025. Accessed: Jan. 28, 2025. [Online]. Available: https://www.hackmageddon.com/category/security/cyber-attacks-statistics/.

[22] Committee on Payments and Market Infrastructures, "Correspondent banking," Bank for International Settlements, Basel, Switzerland, Rep. 147, 2016. Accessed: Jun. 02, 2025. [Online]. Available: https://www.bis.org/cpmi/publ/d147.pdf.

[23] J. Dagher, "PayPal's place in FinTech: From industry pioneer to modern innovator," *SSRN Electron. J.*, Mar. 2025, doi:10.2139/ssrn.5196512.

[24] S. Q. Liu and A. S. Mattila, "Apple Pay: Coolness and embarrassment in the service encounter," *Int. J. Hosp. Manag.*, vol. 78, pp. 268–275, Apr. 2019, doi: 10.1016/j.ijhm.2018.09.009.

[25] Statista, "Apple Pay use by country 2023," Statista, 2023. Accessed: Oct. 05, 2023. [Online]. Available: https://www.statista.com/statistics/1264671/global-apple-pay-adoption/.

[26] Apple Inc., "Apple platform security," Apple Inc., Cupertino, CA, USA, Dec. 2024. [Online]. Available: https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf.

[27] EMVCo LLC, "EMV contactless specifications for payment systems book A: Architecture and general requirements version 2.11," EMVCo LLC, Jun. 2023. Accessed: Jun. 03, 2025. [Online]. Available: https://www.emvco.com/specifications/book-a-architecture-and-general-requirements-11/.

[28] Ripple, "Cross-border payment settlement solution," Ripple, 2023. Accessed: May 31, 2023. [Online]. Available: https://ripple.com/solutions/cross-border-payments/.

[29] Digital Dollar Project, "Exploring a U.S. central bank digital currency: Whitepaper 2.0," Digital Dollar Project, 2023. [Online]. Available: https://digitaldollarproject.org/wp-content/uploads/2023/01/DDP-Whitepaper-2.0_2023.pdf.

[30] B. Chase and E. MacBrough, "Analysis of the XRP Ledger consensus protocol," *arXiv:1802.07242*, Feb. 2018. [Online]. Available: https://arxiv.org/abs/1802.07242.

[31] R. Dongol and J. M. Chatterjee, "Robust security framework for mitigating cyber threats in banking payment system: A study of Nepal," *LBEF Res. J. Sci., Technol. Manag.*, vol. 1, no. 1, pp. 46–83, 2019.

[32] M. Deng, K. Wuyts, R. Scandariato, B. Preneel, and W. Joosen, "A privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements," *Requir. Eng.*, vol. 16, no. 1, pp. 3–32, Oct. 2011, doi: 10.1007/s00766-010-0115-7.

[33] W. Mbaka and K. Tuma, "On the measures of success in replication of controlled experiments with STRIDE," *Int. J. Softw. Eng. Knowl. Eng.*, vol. 34, no. 4, pp. 623–650, Apr. 2024, doi:10.1142/S0218194023500651.

[34] C. B. Simmons, C. Ellis, S. G. Shiva, D. Dasgupta, and Q. Wu, "AVOIDIT: A cyber attack taxonomy," Univ. Memphis, Memphis, TN, USA, Tech. Rep. UMCIS-2009-01, Aug. 2009. [Online]. Available: https://nsarchive.gwu.edu/sites/default/files/documents/4530310/Chris-Simmons-Charles-Ellis-Sajjan-Shiva.pdf.

[35] N. I. C. Mat, N. Jamil, Y. Yusoff, and M. L. M. Kiah, "A systematic literature review on advanced persistent threat behaviors and its detection strategy," *J. Cybersecurity*, vol. 10, no. 1, pp. 1–18, Jan. 2024, doi: 10.1093/cybsec/tyad023.

[36] P. Wooldridge, "BIS quarterly review, March 2020," Bank for International Settlements, Basel, Switzerland, Mar. 2020. [Online]. Available: https://www.bis.org/publ/qtrpdf/r_qt2003.pdf.

[37] ISO, *Information technology - Security techniques - Information security management systems - Requirements*, ISO/IEC 27001:2022, 2022.

[38] D. Temoshok *et al.*, "Digital identity guidelines: Identity proofing and enrollment," Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, NIST Spec. Publ. 800-63A-4, Jul. 2025, doi: 10.6028/NIST.SP.800-63A-4.