Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Securing the Next Generation of Digital Payments: A Threat Model for Virtual Card Ecosystems

Utham Kumar Anugula Sethupathy
Independent Researcher, Senior IEEE Member, Alumni, Nanyang Technological University, Atlanta, USA
Vijayanand Ananthanarayanan
Independent Researcher, Alumni, Fairleigh Dickinson University, Atlanta, USA
Corresponding Author: Utham Kumar Anugula Sethupathy, **E-mail**: mailuthamkumar@gmail.com

| ABSTRACT
The rapid adoption of virtual cards in business-to-business (B2B) payments has created a complex digital ecosystem involving buyers, suppliers, issuers, acquirers, and increasingly, automated processing platforms. While virtual cards offer inherent security benefits, the ecosystem's interconnectedness and reliance on digital channels introduce a new and expanded attack surface. This paper presents a comprehensive threat model for this next generation of digital payments. Using the STRIDE framework, we systematically analyze the security threats inherent in the end-to-end virtual card lifecycle, with a particular focus on novel attack vectors targeting the automated data ingestion and processing stages of platforms like Visa AR Manager. Based on this analysis, we propose a multi-layered, defense-in-depth mitigation strategy. This strategy integrates foundational controls such as PCI DSS compliance, technical solutions including payment tokenization and secure API gateways, and advanced AI-powered fraud detection to create a resilient and secure virtual payment environment capable of withstanding modern threats.

| KEYWORDS

Next Generation of Digital Payments; Threat Model; Virtual Card Ecosystems

| ARTICLE INFORMATION

ACCEPTED: 02 May 2024 **PUBLISHED:** 20 May 2024 **DOI:** 10.32996/jcsts.2024.6.2.27

1. Introduction: The Expanding Attack Surface of Virtual Payments

Virtual cards, which are temporary or limited-use payment credentials, represent a significant evolution in payment security. By design, they reduce risk compared to physical cards; their use can be restricted to specific merchants or spending limits, and a compromised virtual card number does not expose the underlying primary account.[64] This has fueled their rapid growth in the B2B sector, where security and control are paramount.[8]

However, this shift to virtual credentials has transformed the security landscape. Instead of a physical point-of-sale, the attack surface is now a distributed digital ecosystem of email servers, web portals, APIs, and automated backend systems. This complexity introduces new vulnerabilities that are not present in traditional card-present transactions. The increasing sophistication of cyber threats—including advanced phishing campaigns, malware designed to intercept data, and account takeover attacks—poses a significant risk to this ecosystem.[66] The very automation designed to streamline these payments can, if not properly secured, become a vector for large-scale fraud. This paper argues that a formal, systematic threat modeling approach is essential to fully understand and mitigate the unique risks of the modern virtual card payment lifecycle.

2. The Virtual Card Payment Ecosystem: A Component Analysis

To effectively model threats, the system under analysis must first be deconstructed into its core components, data flows, and trust boundaries. The B2B virtual card ecosystem is a multi-party system with several key actors and assets.

2.1 Actors and Assets

- **Actors:** The primary participants in a virtual card transaction include:
  - **Buyer:** The entity initiating the payment.
  - **Supplier (Merchant):** The entity receiving the payment.
  - **Issuing Bank:** The financial institution that issues the virtual card to the buyer.
  - **Acquiring Bank:** The supplier's bank that processes the payment.
  - **Payment Network:** The central infrastructure connecting the banks (e.g., Visa, Mastercard).
  - **AR Automation Platform:** An intermediary service, such as Visa AR Manager, that automates the receipt and processing of the payment on behalf of the supplier.
- **Assets:** The critical data and system components that must be protected include:
  - **Payment Credentials:** Primary Account Number (PAN), Virtual Card Number (VCN), Card Verification Value (CVV), Expiration Date.
  - **Transactional Data:** Invoice data (number, amount, line items), remittance information.
  - **System Data:** ERP system records, user credentials for payment portals and platforms, and audit logs.[69]
  - **Table 1 summarizes the major components of the virtual card ecosystem, the critical assets associated with each component, and their relative security sensitivity. AR automation platforms and ERP systems represent the most critical security zones due to their access to high-value transactional and reconciliation data.**

Table 1 — Virtual Card Ecosystem Components and Assets

Component	Critical Assets	Security Sensitivity
Buyer Portal	Credentials, VCN request	High
Supplier Portal	Invoice data, payment data	High
AR Platform	VCN ingestion, reconciliation	Critical
ERP System	Financial records	Critical
Payment Gateway	Authorization requests	Critical

2.2 Data Flows and Trust Boundaries

A typical automated virtual card transaction follows a multi-stage data flow, which can be visualized in a Data Flow Diagram (DFD). Key trust boundaries—points where data moves from a more trusted to a less trusted environment or vice versa—must be identified as they are often where vulnerabilities lie.

- **Flow 1: Issuance.** The buyer requests a VCN from their issuing bank, typically via a secure online portal.
- **Flow 2: Transmission.** The buyer transmits the VCN and associated invoice details to the supplier. This is often a weak link, frequently occurring over less secure channels like email.

- **Flow 3: Ingestion & Processing.** The supplier's AR automation platform ingests the payment data. This is a critical trust boundary, as the platform must process data originating from an external, potentially untrusted source (e.g., an email server).[24]
- **Flow 4: Authorization & Clearing.** The AR platform securely submits the transaction details to the acquiring bank and payment network for processing.[24] This flow occurs over established, secure payment rails.
- **Flow 5: Reconciliation.** The platform sends structured reconciliation data back to the supplier's internal ERP system, often via a secure API.[24]

Figure 1 illustrates the end-to-end architecture of the virtual card payment ecosystem, highlighting the primary actors, transaction flow stages, and critical trust boundaries where data transitions between secure internal systems and potentially vulnerable external channels. The transmission stage, particularly email-based VCN delivery, represents one of the most significant weak links in the overall security model.

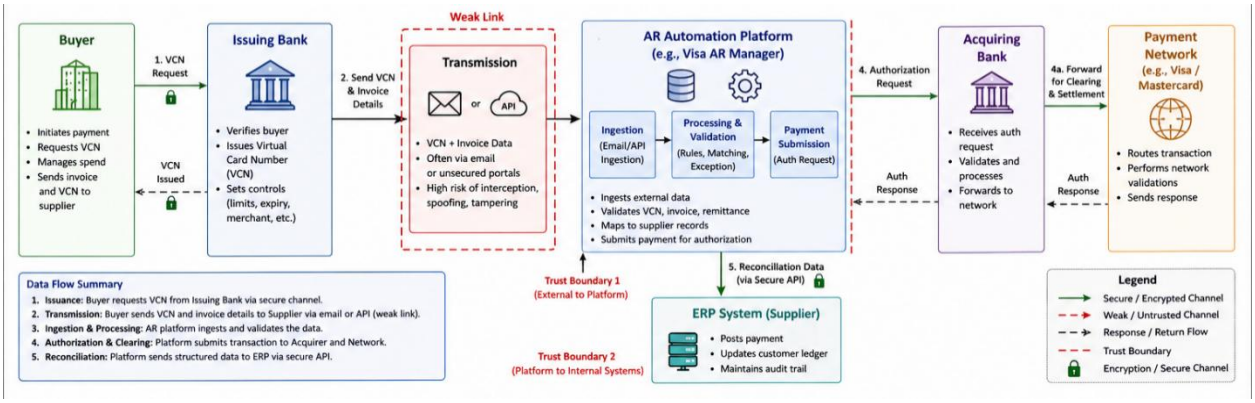

Figure 1. End-to-End Architecture of the Virtual Card Payment Ecosystem and Trust Boundaries

3. Applying the STRIDE Framework to Virtual Card Payments

Using the STRIDE threat modeling framework—which categorizes threats into Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege—we can systematically analyze the risks within the virtual card ecosystem.[70]

A central finding of this analysis is that the automation of VCN ingestion, while solving the problem of manual labor, creates a critical new attack surface. In a manual system, the risk of processing a fraudulent VCN is limited by the speed and diligence of a human employee. In an automated system, an adversary who compromises a supplier's email account can potentially inject fraudulent or tampered payment data at scale, knowing the system is designed to trust and process it automatically. This shifts a primary point of vulnerability from the payment gateway itself to the initial data input channel, making the integrity of that channel paramount to the security of the entire system. As shown in Figure 2, STRIDE threats are not uniformly distributed across the payment lifecycle. The highest concentration of risk occurs during credential transmission and automated ingestion, where spoofing, tampering, and information disclosure threats become significantly more prominent due to external data handling and limited initial trust validation.

STRIDE Category	Virtual Card Transaction Lifecycle Stages					Overall Risk Level
	1. Card Issuance (Buyer ↔ Issuing Bank)	2. Credential Transmission (Buyer → Supplier)	3. Automated Ingestion & Processing (AR Platform)	4. Authorization & Clearing (AR Platform → Network)	5. ERP Reconciliation (Platform → ERP)	
S Spoofing	Medium	High	High	Medium	Medium	High
T Tampering	Low	High	High	Medium	Medium	High
R Repudiation	Low	Medium	Medium	Low	Low	Medium
I Information Disclosure	Medium	High	High	Medium	Medium	High
D Denial of Service	Low	Medium	High	Medium	Medium	Medium–High
E Elevation of Privilege	Low	Medium	High	Medium	Medium	High

Risk Legend: Low (Minimal) | Medium (Moderate) | High (Significant) | Medium–High (Elevated)

Figure 2 — STRIDE Threat Mapping Across Payment Lifecycle

3.1 Spoofing Threats

- **Description:** An attacker impersonates a legitimate entity.[70]
- **Threat Scenario:** An attacker, having compromised a legitimate buyer's email account or using a deceptively similar domain (phishing), sends an email to a supplier containing a fraudulent VCN. The supplier's automated AR system ingests and attempts to process this payment, potentially against a fake invoice.
- **Impact:** Financial loss for the supplier if the payment fails after goods are shipped, or for the legitimate buyer if their identity is used for fraud.

3.2 Tampering Threats

- **Description:** An attacker maliciously modifies data in transit or at rest.[70]
- **Threat Scenario:** An attacker with man-in-the-middle access to a supplier's email server intercepts an incoming payment notification and alters the remittance data to associate the payment with a fraudulent invoice or modifies the VCN details. Alternatively, a malicious insider with access to the payment processing system could alter a batch payment file to redirect funds to their own account.[72]
- **Impact:** Data integrity loss, misapplication of funds, financial theft, and corrupted financial records.

3.3 Repudiation Threats

- **Description:** An attacker (or a legitimate but dishonest user) denies having performed a malicious action because the system cannot prove otherwise.[70]
- **Threat Scenario:** A legitimate buyer authorizes a virtual card payment for a service but later disputes the charge, claiming they never authorized it. Without robust, tamper-evident audit logs that trace the transaction from the initial VCN transmission to the final settlement, the supplier may be unable to prove the transaction's legitimacy and suffer a chargeback.
- **Impact:** Financial loss from chargebacks, increased dispute resolution costs.

3.4 Information Disclosure Threats

- **Description:** Sensitive information is exposed to unauthorized individuals.[71]
- **Threat Scenario:** VCN details (number, CVV, expiry) are transmitted in an unencrypted email and intercepted by an attacker. This could occur via a man-in-the-middle attack on the network or through a data breach of the supplier's email server.[64] Another vector is the misconfiguration of cloud storage, such as a publicly exposed Amazon S3 bucket containing billing logs or transaction data.[69]
- **Impact:** The leaked VCN can be used for fraudulent card-not-present (CNP) transactions, leading to direct financial loss and reputational damage.

3.5 Denial of Service (DoS) Threats

- **Description:** An attacker renders a system or service unavailable to legitimate users.[71]
- **Threat Scenario:** An attacker floods the AR automation platform's public-facing API or the payment gateway with a high volume of junk requests. This can overwhelm the system, preventing it from processing legitimate incoming virtual card payments and disrupting the supplier's cash flow.
- **Impact:** Operational disruption, delayed revenue collection, and reputational damage.

3.6 Elevation of Privilege Threats

- **Description:** An attacker with limited access gains higher-level permissions.[59]
- **Threat Scenario:** An attacker uses a phishing email to steal the credentials of a low-level AR clerk at a supplier company. Using these credentials, they log into the AR automation platform. They then exploit a vulnerability in the

platform (e.g., insecure direct object reference) to escalate their privileges to an administrator level, giving them the ability to view, modify, or redirect all payments processed by the supplier. This is a form of account takeover.[66]

- **Impact:** Complete compromise of the payment system, large-scale financial fraud, and major data breach.

4. A Multi-Layered Defense-in-Depth Mitigation Strategy

No single control can defend against all identified threats. A robust security posture requires a defense-in-depth strategy that layers multiple controls across the ecosystem. **Table 2 maps the layered security controls to the corresponding STRIDE threat categories, demonstrating how foundational compliance measures, technical safeguards, and AI-driven adaptive defenses collectively strengthen the resilience of the payment ecosystem.**

Table 2 — Security Control Layers and Mapped Threats

Security Layer	Technology	Threats Mitigated
Foundational	PCI DSS, Encryption	I, T
Technical	Tokenization, API Security	I, T, D
Advanced	AI Fraud Detection	S, T, E
Operational	Employee Training	S, E

Table 3 presents the detailed STRIDE threat analysis across the virtual card ecosystem, identifying specific attack scenarios, affected assets, business impact, and the most effective mitigation strategies for each threat category. This structured analysis forms the basis for the defense-in-depth strategy proposed in this paper.

Table 3: STRIDE Threat Analysis of the Virtual Card Ecosystem

STRIDE Category	Threat Description	Asset at Risk	Potential Impact	Mitigation Strategy	Source(s)
Spoofing	Attacker impersonates a legitimate buyer and sends a fraudulent VCN to a supplier via a compromised or look-alike email address.	Supplier's AR system, Buyer's reputation.	Financial loss from unpaid goods/services, processing fraudulent transactions.	AI-based behavioral analysis to detect deviations from normal buyer patterns; Transaction velocity monitoring; Multi-factor authentication (MFA) for portal access.	[70]
Tampering	An attacker with man-in-the-middle access alters VCN details (amount, currency) in an email. An insider modifies a batch payment file to redirect funds.	Payment data in transit, payment files at rest, ERP data integrity.	Direct financial theft, corrupted financial records, reconciliation failures.	End-to-end encryption (TLS, AES-256); Payment tokenization to render data useless if intercepted; Strict Role-Based Access Control (RBAC) and immutable audit logs.	[70]
Repudiation	A legitimate customer makes a valid purchase but	Transaction records, audit logs.	Financial loss due to chargebacks, increased dispute	Implement tamper-evident, centralized logging for the entire	[59]

	later disputes the charge, claiming it was unauthorized.		resolution costs.	transaction lifecycle; Use digital signatures for high-value transactions.	
Information Disclosure	VCN and invoice data are leaked from an insecure email server, a data breach at the supplier, or a publicly exposed cloud storage bucket.	VCN details (PAN, CVV, expiry), Personally Identifiable Information (PII), invoice data.	Card-Not-Present (CNP) fraud, identity theft, competitive disadvantage, regulatory fines.	Enforce strong encryption at rest and in transit; Implement payment tokenization to de-risk data storage; Regular cloud security configuration audits.	[64]
Denial of Service (DoS)	Attacker floods the AR automation platform's API or the payment gateway with excessive requests, preventing legitimate transactions.	Service availability of the AR platform and payment gateway.	Disruption of business operations, delayed cash flow, reputational damage.	Implement API rate limiting and throttling; Use a Web Application Firewall (WAF) with DDoS protection; Design scalable cloud architecture.	[69]
Elevation of Privilege	An attacker uses stolen low-level credentials (via phishing) to access the AR platform and exploits a vulnerability to gain admin rights.	User accounts, AR platform administrative functions.	Full compromise of the payment system, ability to alter or redirect all payments, large-scale data breach.	Enforce MFA universally; Adhere to the principle of least privilege with strict RBAC; Regular vulnerability scanning and penetration testing of the platform.	[69]

4.1 Foundational Controls: Compliance and Encryption

- **PCI DSS Compliance:** As a foundational requirement, all entities that store, process, or transmit cardholder data must demonstrate compliance with the Payment Card Industry Data Security Standard (PCI DSS).[74] This standard mandates a baseline of technical and operational controls, including building and maintaining a secure network, protecting cardholder data, implementing strong access control measures, and regularly monitoring and testing networks. For organizations using virtual terminals, this often involves completing the SAQ C-VT (Self-Assessment Questionnaire for Virtual Terminals).[76]
- **End-to-End Encryption:** To mitigate information disclosure threats, all sensitive data must be encrypted both in transit (using strong protocols like TLS 1.2+) and at rest (using robust algorithms like AES-256).[59] This ensures that even if data is intercepted, it remains unreadable to unauthorized parties.

4.2 Technical Controls: Tokenization and Secure API Gateways

- **Payment Tokenization:** Tokenization is one of the most effective controls for protecting payment data. This process replaces the sensitive VCN with a unique, non-sensitive value called a token.[78] The actual card number is stored securely in an isolated, highly protected "token vault," typically managed by a payment service provider. The token itself has no intrinsic value and cannot be mathematically reversed to obtain the original card number.[79] By using tokens throughout

the payment workflow, the risk of data exposure from a breach is dramatically reduced, as the compromised data is useless to attackers.[72] This is a critical mitigation for information disclosure threats.

- **Secure API Design:** The APIs that connect the various components of the ecosystem (e.g., buyer portal to AR platform, AR platform to ERP) are critical control points. These APIs must be secured using best practices, including strong authentication (e.g., OAuth 2.0), granular authorization to enforce least privilege, strict input validation to prevent injection attacks, and rate limiting to defend against DoS and brute-force attacks.[45]

4.3 Advanced Controls: AI-Powered Fraud Detection

- **Behavioral Analytics and Anomaly Detection:** To counter sophisticated spoofing and tampering attacks, systems must move beyond static rules. AI and machine learning models can establish a baseline of normal transactional behavior for each customer and supplier. They can then monitor transactions in real-time, flagging anomalies that may indicate fraud—for example, a transaction from an unusual geographic location, a VCN used outside of its intended merchant category, or a sudden spike in payment frequency.[80]
- **Dynamic Risk Scoring:** Instead of a simple pass/fail check, AI models can assign a dynamic risk score to each transaction based on hundreds of variables, including device fingerprinting, IP reputation, transaction velocity, and historical patterns.[33] Transactions with high risk scores can be subjected to additional scrutiny or require step-up authentication, providing a more nuanced and effective defense.
- **Insider Threat Detection:** AI models can also be trained to monitor internal user activity logs. By identifying deviations from normal behavior—such as an employee accessing payment data at an unusual time or attempting to export large volumes of records—these systems can help mitigate the significant risk posed by malicious or negligent insiders.[67]

5. Discussion: Balancing Security, Usability, and Scalability

Implementing these security controls involves navigating inherent trade-offs. Overly stringent security measures can introduce friction for legitimate users, degrading the customer experience. For example, requiring complex multi-factor authentication for every minor action can frustrate users and hinder adoption. Conversely, prioritizing a frictionless experience can open security gaps.

Platforms like Visa AR Manager represent an effort to strike this balance by abstracting much of the security complexity away from the end-user. By providing a secure-by-design processing environment, they allow suppliers to benefit from automation without needing to become security experts themselves. Nonetheless, non-technical controls remain critical. Regular employee training on cybersecurity best practices, particularly on how to identify and report phishing and other social engineering attempts, is essential, as the human element often remains the weakest link in the security chain.[67]

6. Conclusion

The B2B virtual card ecosystem, while offering significant benefits in efficiency and control, presents a complex and attractive target for cyber adversaries. A systematic threat analysis using the STRIDE framework reveals critical vulnerabilities at multiple points in the transaction lifecycle, with the automation of data ingestion creating a particularly potent new attack vector. Securing this next generation of digital payments requires a robust, defense-in-depth strategy. This strategy cannot rely on a single solution but must layer foundational compliance frameworks like PCI DSS, strong technical controls such as payment tokenization, and advanced, adaptive defenses powered by AI-driven fraud detection. By understanding the threats and implementing a multi-layered security architecture, the financial industry can foster a payment ecosystem that is not only efficient and scalable but also resilient and trustworthy.

Table 3 presents the detailed STRIDE threat analysis across the virtual card ecosystem, identifying specific attack scenarios, affected assets, business impact, and the most effective mitigation strategies for each threat category. This structured analysis forms the basis for the defense-in-depth strategy proposed in this paper.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.

References

[1] Visa AR Manager: Remove the friction associated with accepting virtual cards. Visa. Available at: https://usa.visa.com/products/ar-manager.html
[2] Visa Announces the General Availability of Visa AR Manager in the U.S. Visa. Available at: https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.21446.html
[3] Visa Launches AR Manager Tool, Targeting Suppliers' Biggest Business Payments Bottleneck. PYMNTS. Available at: https://www.pymnts.com/accounts-receivable/2025/visa-launches-ar-manager-tool-targeting-suppliers-biggest-business-payments-bottleneck/
[4] Virtual Card Numbers and SDP Compliance FAQs. Mastercard. Available at: Mastercard documentation PDF
[5] Payment Card Industry Security Standards Council. Payment Card Industry Data Security Standard (PCI DSS). Available at: https://www.pcisecuritystandards.org/standards/
[6] STRIDE Threat Model: A Complete Guide. Jit.io. Available at: https://www.jit.io/resources/app-security/stride-threat-model-a-complete-guide
[7] Threat Modelling 102: Applying STRIDE to Payments Architecture. Available at: https://infosecwriteups.com/threat-modeling-102-applying-stride-to-payments-architecture-f0f542fc1698
[8] What Is the STRIDE Threat Model? Pure Storage. Available at: https://www.purestorage.com/knowledge/stride-threat-model.html
[9] How Tokenization Transforms B2B Payment Security. Bottomline Technologies. Available at: https://www.bottomline.com/resources/blog/how-tokenization-transforms-b2b-payment-security
[10] Payment Tokenization 101: What It Is and How It Benefits Businesses. Stripe. Available at: https://stripe.com/resources/more/payment-tokenization-101
[11] AI Fraud Detection in Banking. IBM. Available at: https://www.ibm.com/think/topics/ai-fraud-detection-in-banking
[12] How Machine Learning Works for Payment Fraud Detection and Prevention. Stripe. Available at: https://stripe.com/resources/more/how-machine-learning-works-for-payment-fraud-detection-and-prevention
[13] Mitigating Cyber Threats in Digital Payments: Key Measures and Implementation Strategies. PhilArchive.
[14] Securing FinTech and Digital Payments: Identifying Threats, Mitigating Vulnerabilities, and Strengthening Defenses. ResearchGate.