Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Securing Payment Transactions in a connected world - IoT

Kishore Bellamkonda Sunderajulu

Payments Fintech Leader, kishorebs83@outlook.com

Ensuring payment integrity is crucial to fostering trust among customers, merchants, and payment service providers. A robust encryption solution is key to safeguarding transactions against eavesdropping, replay attacks, and data tampering. By addressing vulnerabilities and preventing data compromise, such solutions enhance transaction integrity, bolster user confidence, and protect identity within the payment ecosystem.
In an era of escalating compliance demands from regulators, the development of scalable security frameworks becomes increasingly imperative. These frameworks must seamlessly integrate across diverse IoT devices, ensuring universal protection and adaptability. A comprehensive, forward-looking approach to payment security not only mitigates risks but also strengthens the foundation of modern digital transactions, enabling secure and seamless financial interactions across connected ecosystems.

1. Introduction

The dynamic evolution of digital payment systems has brought unprecedented convenience but also heightened the need for robust security measures. This paper delves into the pivotal role of real-time, scalable cryptographic solutions in safeguarding payment integrity and enhancing merchant operations. By mitigating risks such as fraud and chargeback liability, these solutions not only provide a safer payment ecosystem but also bolster economic resilience.

Furthermore, scalable cryptographic frameworks foster digital financial inclusion by ensuring secure transactions across diverse platforms and encouraging innovation in payment technologies. As the Internet of Things (IoT) continues to transform transactional landscapes, these solutions emerge as a cornerstone for securing IoT-enabled payments, paving the way for a more secure and inclusive digital future

The customer journey experience in the Internet of Things (IoT) ecosystem revolves around seamless connectivity, personalization, and convenience. It typically begins with the discovery phase, where customers identify a need or desire for an IoT solution, such as smart home devices, wearable technology, or industrial IoT applications. This is followed by the onboarding phase, where users purchase, set up, and integrate IoT devices with existing systems, often requiring intuitive apps or platforms.

During the usage phase, customers interact with the device, experiencing real-time data collection, automation, and personalized insights. Key touchpoints include smooth connectivity, ease of use, and reliability of device performance. IoT solutions often include proactive features, like predictive maintenance or automated alerts, which enhance user satisfaction.

The journey extends to the support phase, where customers expect quick resolutions for technical issues, software updates, and continuous improvements. Privacy and data security are critical concerns throughout the experience, as users entrust IoT systems with sensitive information.

Ultimately, a successful IoT user journey is marked by a cohesive experience that adapts to user needs, builds trust, and fosters loyalty through consistent value delivery

2. Problem Statement

While IoT devices offer advanced security features such as voice recognition, biometric validation, device binding, and 3DS authentication to authenticate users and protect payment credentials, vulnerabilities remain in ensuring data integrity during critical processes like pre-authorization and authorization. Threats such as skimming, man-in-the-middle (MITM) attacks, and replay attacks pose significant risks despite these safeguards. To address these challenges, a robust cryptogram-based approach is essential to secure sensitive data and uphold the integrity of transactions within the IoT ecosystem. Let's review the User journey aka User experience.

3. User journey

Step-by-Step Process for Secure Payment Transaction Flow:

1. Customer Checkout Initiation:

The customer places an order using a mobile app or eCommerce browser and navigates to the checkout page.

2. Merchant Captures Checkout Information:

The merchant's browser captures payload credentials and associated checkout information (e.g., card details, transaction amount, merchant identity) and forwards them to their acquirer processor.

3. Acquirer Processor API Request:

The acquirer processor sends a payload request to the payment service provider via an API, secured by a TLS connection with JSON Web Encryption (JWE) keys.

4. Payload Decryption and Unique ID Generation:

The encrypted payload is decrypted, and a cryptogram is generated. A 4-byte hexadecimal unique ID is created in the hosting database, leveraging merchant credentials and an incremental value linked to the card number.

5. Token Validation (if Applicable):

If the payment involves a tokenized card number, the token vault is called to detokenize and retrieve the real PAN (Primary Account Number).

Network proprietary rules associated with token credential validation, established during token creation, are applied.

6. Data Concatenation for Hex Object:

The merchant-provided payload data, customer credentials, and network proprietary data are concatenated to generate a hex data object.

7. Cryptogram Generation:

An HSM command for Authorization Request Cryptogram used in EMV chip card processing is used to generate a cryptogram.

The cryptogram is based on the payload data and the payment service provider's proprietary cryptogram algorithm, using 3DES or AES encryption standards.

8. Cryptogram Submission to Merchant:

The generated cryptogram is sent back to the merchant for inclusion in the authorization flow, conforming to the ISO 8583 message format.

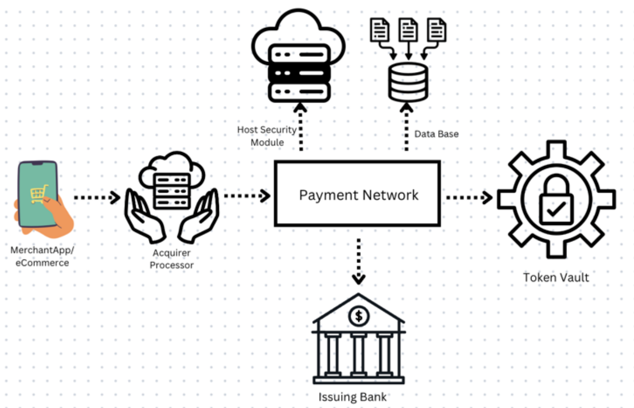
9. Cryptogram Validation during Authorization:

The ISO message received during the authorization process is parsed, and the payload details are used to call the HSM for cryptogram validation.

10. Dynamic Cryptogram Validation:

Using the data provided in the ISO message, the system validates the merchant data and unique identifier. The incremental counter is checked to ensure the cryptogram's one-time authenticity, confirming that the dynamic cryptogram is unique to the transaction.

4. Systematic flow



5. Cryptogram generation process

Payload credentials as part of the API or mobile device app request may contain the following:

Card or token number, expiry date, MCC code, Merchant credentials i.e merchant name/location, POS device ID, eCommerce ID, UUID, merchant ID, URL. In addition merchant captures customer checkout details and submits them as part of the payload request Amount and Transaction Currency code.

Leveraging the merchant-provided details, the payment service provider may use their proprietary fields like incremental transaction counters associated with the card or token number. Generate a unique dynamic number or identifier hosting the merchant credentials with 4 bytes hex data and use amount and APP ID or eCommerce ID appended to the Amount to generate a 8 digit data.

Sample data:

Amount : 000000001200

Incremental Counter : 0015

Transaction Currency code : 0840

Payment service providers proprietary data: 0119000000001200 (App ID + Amount)

Unique ID – 4A13BEFE (merchant name or POS device ID, eCommerce ID, UUID, merchant ID,URL)

Using the 3DES and AES encryption standard with issuing Bank proprietary issuer master key (encrypted under double or triple length key)

Key example :

A1 - 12AAE125890AFF12 (key 1)

A2 - FAEECB169812012F (key 2)

Combined Key A3= A1+A2 12AAE125890AFF12FAEECB169812012F

Card or Token number: 9910001245678901

Sequence number of the card : 000 (for primary card, if secondary, card sequence number can be 001,002,etc)

ML = Card number + Sequence number = 1000124567890100

MR = ML XOR FFFFFFFFFFFFFFFF = EFFFEDBA9876FEFF

Using DES encryption,

MK L = des(A3,ML) = E384CC177C7AB4D2

MK R = des(A3,MR) = FDB6A20C59DA7F1A

MK = MK L + MK R

E384CC177C7AB4D2FDB6A20C59DA7F1A

Incremental counter = 0015

Concatenate = Incremental Counter+000000000000

= 0015000000000000 (multiple of 8)

RL = 0015F00000000000 (incremental counter+padding)

RR = 00150F0000000000 (incremental counter+padding)

Unique Key A = des(MK,RL)

= B80129D0467CEA22

Unique Key B = des(MK,RR)

= 2718D84E2E1ECDE3

Unique Key = Unique Key A + Unique Key B

B80129D0467CEA222718D84E2E1ECDE3

Concatenated Data Objects:

Amount+Transaction Currency Code+Unique ID+Incremental Counter+Payment service providers proprietary data(App ID+Amount)

00000000120008404A13BEFE00150119000000001200

Padding data with 8000 to translate the concatenated data object multiple of 8 therefore break it down into 3 equal data blocks.

00000000120008404A13BEFE001501150000000012008000

D1 = 0000000012000840

D2 = 4A13BEFE00150115

D3 = 0000000012008000

Applying 3DES encryption standard:

O1 = Unique Key A enc D1

= B80129D0467CEA22 (enc) 0000000012000840

= 3C70F9E02A422528

V1 = O1 XOR D2

= 3C70F9E02A422528 XOR 4A13BEFE00150115

= 7663471e2a57243d

O2 = Unique Key A enc V1

= B80129D0467CEA22 enc 7663471e2a57243d

= 0376A8917B3DD6EA

V2 = O2 XOR D3

= 0376A8917B3DD6EA XOR 0000000012008000

= 0376a891693d56ea

O3 = Unique Key A enc V2

= B80129D0467CEA22 enc 0376a891693d56ea

= 31D6D62C8E87AE99

O4 = Unique Key B dec O3 (dec = decryption)

= 2718D84E2E1ECDE3 dec 31D6D62C8E87AE99

= AD872D00E8972440

O5 = Unique Key A enc O4

= B80129D0467CEA22 enc AD872D00E8972440

= ECA8C012F4A49B50

Final Dynamic Cryptogram = ECA8C012F4A49B50

When submitted in the ISO message or API payment validation message along with merchant data that can be linked to the unique identifier (Unique ID) an incremental counter can be detected from any replay of the cryptogram if the same incremental counter is submitted more than once to verify the uniqueness of the cryptogram.

6. Conclusion

In conclusion, the solution ensures payment integrity and compliance with EU and RBI mandates while offering scalability across diverse payment markets and devices, including mobile apps, car play systems, and eCommerce platforms. The solution mitigates disputes and chargeback liabilities, driving increased acceptance and higher approval rates for merchants and building customer trust.

References

Contactless Payments During the Pandemic

- EMVCo. (2021). The Role of Contactless Payments in Ensuring Safety and Security. Retrieved from https://www.emvco.com
- Kishore Bellamkonda Sunderajulu, "Enhancing Payment Transaction Security", International Journal of Science and Research (IJSR), Volume 13 Issue 11, November 2024, pp. 680-684, https://www.ijsr.net/getabstract.php?paperid=SR241110202744, DOI: https://www.doi.org/10.21275/SR241110202744
- Visa. (2020). How Contactless Payments Are Changing Consumer Habits During COVID-19. Retrieved from https://www.visa.com

The Evolution of the Payments Industry

- World Bank. (2022). Digital Financial Services: A Path to Financial Inclusion Post-COVID-19. Retrieved from https://www.worldbank.org

- McKinsey & Company. (2021). How COVID-19 Is Reshaping Global Payments. Retrieved from https://www.mckinsey.com

Future Trends in Payments

- Capgemini. (2023). World Payments Report 2023. Retrieved from https://www.capgemini.com
- eCommerce & Digital Wallet Payment Fraud - Kishore Bellamkonda Sunderajulu - AIJMR Volume 2, Issue 6, November-December 2024. DOI 10.62127/aijmr.2024.v02i06.1111
- Deloitte. (2022). The Future of Payments: New Technologies and Financial Inclusion. Retrieved from https://www2.deloitte.com

Security Features in Contactless Payments

- PCI Security Standards Council. (2024). Contactless Payments Security Guidelines. Retrieved from https://www.pcisecuritystandards.org
- Mastercard. (2021). Tokenization and Security in Contactless Transactions. Retrieved from https://www.mastercard.com

Impact on Merchants and Consumers

- EY. (2022). COVID-19 and the Shift to Digital Payments: What It Means for Merchants and Consumers. Retrieved from https://www.ey.com
- Accenture. (2021). The Pandemic's Impact on Consumer Payment Preferences. Retrieved from https://www.accenture.com

Retail Agent Banking and Financial Inclusion

- Tanzania Banking Sector Report. (2021). The Role of Retail Agents in Enhancing Financial Inclusion. Retrieved from https://www.tzbankingreport.com

CGAP. (2020). Agent Networks and Their Role in Expanding Financial Access. Retrieved from https://www.cgap.org