GlobalLogic®

Reducing Threats In Retail

Authored by
Prageet Pathak
Yashasvi Kalra

Contents

Introduction 1

Data Transactions in Retail 2

Threats in Retail Transactions 3

Proposed Solutions—Encryption Techniques 4

- Encryption
- Importance of Encryption
- Methods of Encryption

Data Security—Applications of Encryption 6

- Payment Security
- Network Security
- Cloud Hosting And Database Security

Future Scope 8

- Homomorphic Encryption
- Quantum Encryption

Conclusion 9

References 10

Introduction

Digital technology is evolving rapidly and is now an integral part of our daily lives. Many businesses have adopted and implemented innovative technologies in their business models, and retailers can make the most out of these advancements.

Retailers enhance the customer experience and make shopping more convenient by using innovative tools and technology. Retailers are engaging those customers who like to shop and connect using new and exciting ways. Customers use digital technology to pay for items, and most of these payments are online or offline through point of sale (POS).

Many customers have opted to use digital payment options during the COVID-19 pandemic out of fears of virus transmission from physical currency use. This digital use puts an onus on the industry to protect customer data and payment card details when payment methods are digitized. Retailers also need secure and reliable digital payment solutions.

With a high volume of personally identifiable information (PII) and payment card information (PCI) changing hands with each transaction, the retail business is one of the most vulnerable targets of cyber-attacks.

Many technology options exceed existing requirements for the PCI. Point-to-point encryption (P2PE) and end-to-end encryption (E2EE) can address many vulnerabilities in the payments processing chain. P2PE encryption is a standard established by the PCI Security Standards Council designed to provide a robust security solution for electronic financial transactions, and E2EE can address security weaknesses that exist when cardholder data is captured and processed.

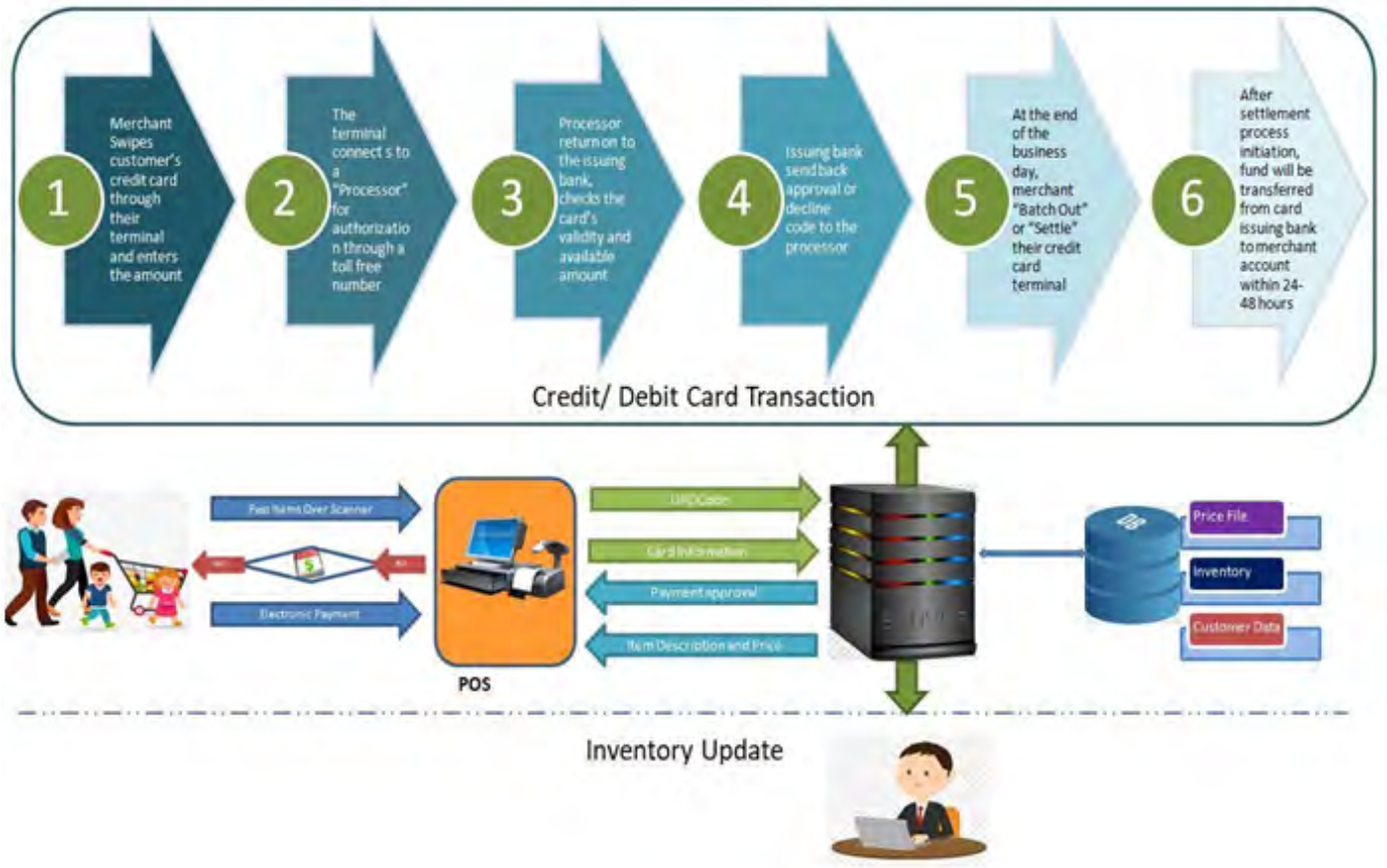
This paper helps merchants understand encryption and how it can be useful in protecting retail transactions.

Data Transactions in Retail

Data in retail is varied, including POS, loyalty card, customer-centric, supply chain, operations and merchandising data. In short, we can define various types of data in retail like sales data, return data, inventory data, operational data, financial transactions data, customer data or promotions data.

In retail, all the data needs to be secured as it travels from one system to another. The customer expects retailers to keep their data safe, regardless of whether it is personal, credit card or any other data type.

Retail - Data Transaction Flow



Threats in Retail Transactions

Retailers need to provide the best service to customers while simultaneously using security best practices in the system to secure data or prevent any unapproved data access or modification.

Here are the major threats in retail transactions.

POS Attacks: PoS digitization has changed the PoS functionality by recording and collecting value-based information. PoS is a significant objective for a scam, affecting everything from in-store retail to web-based business vulnerabilities.

Network Intrusion: Any unauthorized activity on a computer network. Network intrusion hijacks network resources that have different purposes and compromise the security of the system. A Trojan is a popular network intrusion that seems harmless but can delete stored information and open security channels to allow outside hackers into the network.

Unauthorized System Access: The point at which someone outside the system accesses the system or network using another person's account information. Hackers can target users with passwords saved on password managers or signin directly if the user has an easy password. There are also extraordinary measures by which a virus can follow a computer and trace passwords.

Payment Card System Vulnerabilities: These pose considerable retail threats. Unless there is basic point-to-point encryption, the payment card system is exposed to outside attacks. There are also potential buffering errors, where the buyer is charges but the order is not completed through the vendor.

As indicated in the recent study, Cyber Security Mid-Year Snapshot 2019 by Cyber Security Hub, critical infrastructure, phishing scams, and email takeovers are the three most dangerous retail security challenges. Therefore enhancing enterprise security is high on the demand for many small and large businesses.

Proposed Solutions—Encryption Techniques

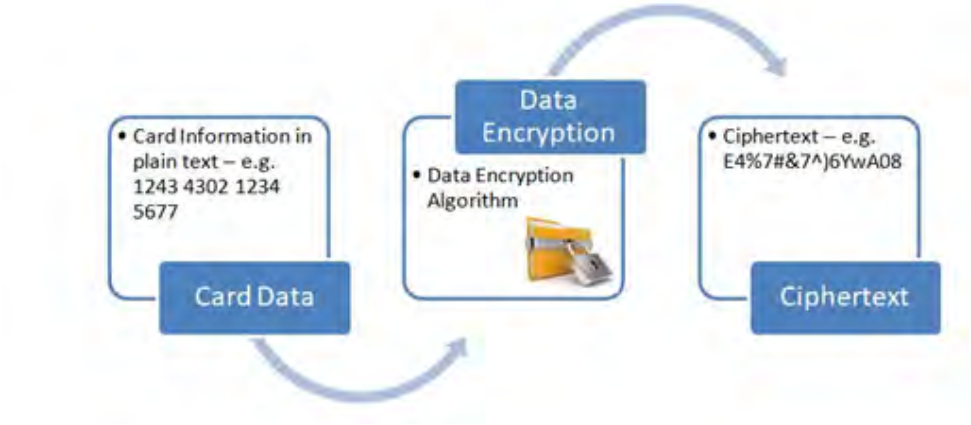
Various solutions can reinforce the security infrastructure of a retailer. Retailers can encrypt data through integrated key management, which makes data unreadable. They can also limit access to encrypted data by changing who has access and controls to the data.

With these safeguards, only authorized users can decrypt the data. Retailers should implement security intelligence that tracks attempts to access the encrypted data, which will provide insights into how external attackers are attempting to breach the security.

- Endpoint protection to prevent attack through Point-of-Sale terminals.
- Encryption to shield data even when it is inside a compact device.

Encryption

Encryption is a procedure of converting plain content data into a non-readable structure called ciphertext. A key is required to decode the data and return it to its original plain content form.



Importance of Encryption

Encryption is utilized to make sure that data in travel and data at rest are secure. Each time someone uses an ATM or buys something on the web with a smartphone or computer, encryption is used to secure the transferred data. Organizations continuously rely upon encryption to shield applications and sensitive data from reputational harm when there is a data breach.

Methods of Encryption

Symmetric encryption is referred to as secret key encryption—a single key is used for both encryption and decryption. The key is considered a "common secret" since both the sender or registering machine doing the encryption must share the secret key to anyone approved to decrypt the data. Symmetric key encryption is a lot quicker than asymmetric encryption. The most broadly utilized symmetric key cipher is the Advanced Encryption Standard (AES), intended to secure government-ordered data.

Asymmetric encryption is also referred to as public-key encryption, which uses two different but logically linked keys. This cryptography frequently employs prime numbers to make keys since it is computationally hard to factor large prime numbers and break the encryption. The Rivest-Shamir-Adleman (RSA) encryption algorithm is, as of now, the most broadly used public-key algorithm. With RSA, private or public keys can encrypt a message, and whichever key isn't utilized for encryption turns into the decryption key.

Hash functions are one way encryptions, scrambling text to produce a unique message digest. There is no way to reverse the process to reveal the original password; hackers must guess the original password to unencrypt the file. A hash function should be computationally proficient (simple to figure), deterministic (dependably creates a similar outcome), preimage-resistant (output doesn't uncover anything about info), and collision-resistant (nearly impossible that two cases will deliver a similar outcome) to be powerful. Popular hashing algorithms incorporate the Secure Hashing Algorithm (SHA-2 and SHA-3) and Message-Digest Algorithm 5 (MD5).

Symmetric Algorithms	Asymmetric Algorithms	Hash Functions
AES	Diffie-Hellman	SHA-1
DES	RSA	SHA-2
Blowfish	Elliptic Curve Cryptography	SHA-3
Twofish	DSS	MD5
3des	Elgamal	BLAK

Data Security—Applications of Encryption

Data security is generally classified based on the state of the data: data at rest, data in motion and data in use. Understanding data security based on different data transaction points helps retailers make informed choices rather than just accepting proposals of their chief technology officers without understanding the options completely. Security solutions used at various data transaction points such as payments, networks, and cloud hosting and databases are discussed below.

Payment Security

Point to Point Encryption (P2PE)

PCI Security Standards Council established the Payment Card Industry Data Security Standard (PCI DSS) to secure electronic financial transactions. P2PE is at the heart of PCI DSS and a must for payment processing systems. Card data is encrypted once as it is swiped at the POS (point of sale) terminal and transmitted in encrypted form to the payment processor. The payment processor decrypts the data at its end and generates authorization tokens for the merchant. In the case of a data breach, third parties cannot decrypt data as they don't have encryption keys and data in this form will be of no use to them.

End to End Encryption (E2EE)

End to End Encryption (E2EE) is considered more secure than P2PE in the payment processing industry. E2EE and P2PE both encrypt data when the card is swiped at POS or point of information (POI). However, P2PE sends encrypted data to the payment processor when data is decrypted and sent to the acquirer through an encrypted tunnel. In contrast, in E2EE, encrypted data is directly sent to the acquirer. Card data is not decrypted at any point and is decrypted directly by the acquirer. P2PE solutions are adopted widely in the payment industry as P2PE components are validated by PCI P2PE assessors, which provides more trust than E2EE solutions for secure payment processing.

Tokenization

Tokenization is a process of replacing sensitive information with randomly generated numbers. For example, a customer's primary credit card account number is replaced by randomly generated numbers called tokens. This technique allows users to store credit card information into mobile wallets, e-commerce solutions and POS software without exposing card information.

EMV

EMV revolutionized the physical payment card industry by using microchips embedded inside payment cards. These chip cards or smart cards are used with a PIN (personal identification number). Sensitive card information like PAN (primary account number), expiry date, customer name and CVV are encoded with standard encryption techniques and stored into microchips when they are personalized.

Network Security

SSL/TLS (Transport Layer Securing)

SSL (secure socket layer) is succeeded by TLS (transport security layer), but this protocol is still referred to as SSL or SSL/TLS. This protocol provides transport layer security for secure communication by authenticating client and server and encryption of data.

HTTPS (Hypertext transfer protocol)

HTTPS is an application of SSL/TLS which makes web browsing secure and provides authenticity, integrity and encryption of data when client and server exchanges sensitive information such as credit card numbers, social security numbers or credentials over the internet. Transmission of such information was not possible earlier by using HTTP protocols.

Cloud Hosting And Database Security

Encryption of Sensitive Data

Sensitive data such as credit card numbers, social security numbers, credentials, and customer data required in an application must be identified and encrypted using standard encryption algorithms before sending it to the database and then later decrypted upon retrieval from the database.

This application-level encryption of sensitive data comes with challenges such as key management, use of standard encryption algorithms and providing a secured environment for encryption devices. Many of these issues can be resolved with encryption as a service (EAAS). However, this solution comes with additional costs.

EAAS (Encryption as a Service)

EAAS is a subscription-based form of cloud service encryption that allows cloud-based applications access to no-overhead setup, easy to use API, efficient performance and cost based on usage. Encryption services can be monitored to check how many times they have been requested, and key business decisions can be made accordingly. Popular services include key vaults for key management, FDE (Full Disk Encryption), cloud storage encryption, database encryption, etc.

Future Scope

Homomorphic Encryption

Strong encryption techniques are available for data at rest and data in transmission. However, little has been examined for data that is in use, which means when data is computed in plain text and is vulnerable to manipulation by attackers. One solution to this problem is homomorphic encryption.

The term “homomorphic” means “having the same structure”. Data in this encryption technique remains encrypted while mathematical computations are done, and results are returned without ever decrypting the data.

A prominent Brazilian financial institution has worked with IBM Research to apply homomorphic encryption on banking data. The pilot showed that it was possible to apply machine learning algorithms on encrypted data without decrypting it. This encryption method is creating a new level of privacy that could be applied to other industries as well.

Quantum Encryption

Quantum cryptography uses the fundamentals of quantum mechanical properties to achieve cryptographic goals and adds innovation in quantum computing. This encryption technique proposes revolutionary solutions for various cryptographic problems which could not be solved by classical methods till now, such as quantum key distribution, detection of eavesdropping, or encryption when data is in use.

Conclusion

P2PE and E2EE solve security weaknesses in traditional methods that could not solve e-payments and retail transactions. P2PE is a strong security solution for electronic money-related exchanges, and E2EE takes care of security weaknesses that exist when cardholder data is captured and processed by the merchant. The use of one or both of these technologies today in retail and digital environments can be used to minimize security threats. Using the two technologies together is a very powerful way to secure data.

Recent data breach cases show that retail merchants don't fully comply with the PCI DSS standard, which results in loss of customer and business data. Therefore, retailers should focus on achieving PCI DSS compliance and use Cloud PAAS service providers like AWS, Azure or GCP to better protect their application and data from attacks. Cloud services provide easy to use infrastructure to build and deploy applications. They provide storage encryption, EaaS (Encryption as service) and FDE system security services.

Looking at the importance of these technologies, retailers must adopt advanced technologies for more secure and robust growth in Industry.

References

TechTarget SearchSecurity

Intellias Intelligent Software Engineering

Square

Marsh

Investopedia

DotActiv

About the Authors

Prageet Pathak is a Senior QA Lead with GlobalLogic contributing to various streams through his automation skills in mobile and web application.

Yashasvi Kalra is an enthusiastic Developer working in financial projects utilizing his Java expertise.

GlobalLogic®

GlobalLogic is a leader in digital product engineering. We help our clients design and build innovative products, platforms, and digital experiences for the modern world. By integrating strategic design, complex engineering, and vertical industry expertise,— we help our clients imagine what's possible and accelerate their transition into tomorrow's digital businesses. Headquartered in Silicon Valley, GlobalLogic operates design studios and engineering centers around the world, extending our deep expertise to customers in the communications, automotive, healthcare, technology, media and entertainment, manufacturing, and semiconductor industries.

www.globallogic.com