Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2023, 10(9):77-86**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

An In-depth Knowledge on EMV Tags and their Adoption in FinTech and Traditional Banking

Pavan Kumar Joshi[1], Rajesh Kotha[2]

[1]Director Information technology, Fiserv, USA
[2]Software Development Engineering Advisor, Fiserv, USA

Abstract: EMV stands as the leading global standard for smart card payments. "EMV transaction specifications are based on a variety of standards, each serving a distinct purpose" [6, p. 17]. Figure 1 depicts such specifications: The EMV specification offers a versatile toolkit for payment protocols, allowing for various combinations of authorization. Its complexity and flexibility make it difficult to thoroughly analyze the security of the EMV standard. This study explored the implementation of "Europay, Mastercard, and Visa" (EMV), prompted by notable cybercrimes [1]. The aim is to shed light on the impact, solutions, and applications of EMV technology. The findings suggest that the increase in data breaches has driven this technological transition. High-profile companies like Target have experienced cyberattacks, resulting in substantial financial losses for numerous U.S. organizations due to data breaches. The technology landscape is particularly susceptible when it comes to processing financial exchanges. EMV bolsters the security level of financial transactions.

Keywords: EMV Technology, Cybersecurity, Financial Transactions, Fraud Prevention, Smart Card Payments, Chip and PIN, Contactless Payments, Data Encryption, Payment Tokenization, EVMco, Banking systems, Mobile Payments, Transaction Security, Fraud Risk.

1. Introduction

Financial transaction systems play a crucial role in facilitating money exchange in market economies. However, these systems also come with vulnerabilities and flaws that heighten their risk. They must fulfill several requirements, including security, acceptability, usability, and cost, each presenting its own advantages and disadvantages. EMV technology was developed to combat fraudulent transactions, but its implementation has proven to be more complex than anticipated. While it offers benefits, EMV also brings new vulnerabilities, such as counterfeit cards. This paper is part of ongoing research examining the effects of EMV tags and chips on the Fintech and banking sectors. The aim is to shed light on the impact, solutions, and applications of EMV technology, as well as how financial institutions can utilize it to address vulnerabilities and shortcomings in financial transaction systems. Besides, conventional magnetic stripe carries data in a manner that might be easy to read. All things considered, EMV chips store the cardholder data on an actual metallic chip which can only be read by specialized devices; thereby raising the security level.

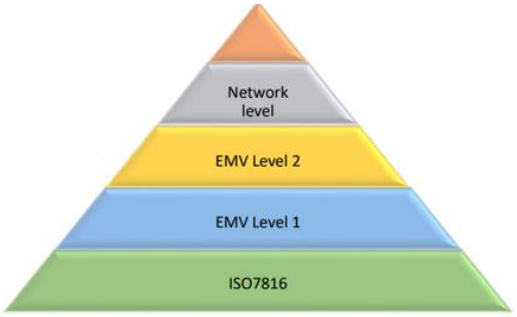

Figure 1: *EMV standards [6].*

2. Scope

Cybercrime is becoming more sophisticated, targeting governments, businesses, and individuals alike [2]. This trend highlights the increasing significance of AI on a global scale. This research paper explores the role of EMV in combating fraud, with a focus on areas such as financial transactions, online shopping, and cybersecurity. It examines "contactless chips, mobile payments, EMV QR Codes, EMV 3D-Secure, Contact Chips" and other types of EMV, which are particularly effective in tackling fraud-related challenges [2]. The paper outlines how AI techniques can uncover features that traditional systems may overlook, allowing for a clear distinction between fraudulent and legitimate transactions. It also discusses the application of EMV to identify areas at risk for fraud and to implement proactive measures. The research addresses the challenges associated with using EMV including data privacy concerns, the quality of datasets, and the interpretability of models. Considering these challenges, the paper assesses the ethical and practical considerations that require attention. Additionally, the research underscores the importance of regularly updating EMV systems to ensure their effectiveness and adaptability during transactions. The paper advocates for further research aimed at developing EMV technologies that bolster fraud prevention, enhance financial systems, minimize misuse, and uphold consumer trust in the digital era.

3. Literature Review

In 1993, Europay, Mastercard, and Visa came together to establish a global standard for secure payment technology aimed at processing credit and debit card transactions. This standard, referred to as EMV, was created to replace older card-present verification methods such as magnetic stripes and mechanical imprints, which had become less effective against sophisticated fraud techniques. Since then, American Express, JCB, and UnionPay have joined the original members to form EMVCo, which is responsible for overseeing EMV payments and continuously developing new specifications to tackle emerging fraud trends and advancements in technology **(Figure 2).** EMV cards are equipped with embedded microchips, which store encrypted data and generate dynamic transaction codes; this increases financial security.

Figure 2: *EMVCO owners [6].*

EMV is a broad system that encompasses different types of payment technology. The first one is EMV Contact Chips [4]: These chips are embedded in cards and require physical contact with a reader. They use encryption to secure transactions, generating a unique code for each transaction to help prevent fraud. The second type is the Contactless Chips: These chips allow for tap-to-pay transactions. Users tap their card or device near the terminal for quick and secure payments. The third type is EMV Mobile Payments. Smartphones or wearables equipped with NFC technology enable secure, contactless transactions [10]. Mobile wallets store card information and create unique transaction codes for each payment. The fourth type is the payments tokenization, which replaces sensitive card details with a unique token during transactions. This token becomes useless if intercepted, significantly enhancing security for mobile and online payments.

Another type of EMV is the EMV QR Codes, [3] depicted by **Figure 3.** Standardized QR codes let consumers scan with their mobile device to complete transactions. This method accommodates both card-based and account-based payments. The sixth approach is the secure remote commerce. These standard streamlines online checkouts by offering a consistent and secure experience across various websites and apps. Consumers can use a single sign-in to securely store and manage their payment information. The last type is the EMV 3D Secure, which adds the authentication level for finances. It facilitates data exchange between the merchant and issuer to verify the cardholder's identity, reducing fraud and ensuring secure e-commerce payments.

Figure 3: *Example of market level QR [5].*

The whole process of EMV transactions take a few seconds and here is how it works. As depicted by Figure 4 A cardholder initiates a transaction by either inserting their EMV chip card into a payment terminal. After identity is confirmed, the EMV chip generates a unique, one-time transaction code and sends this cryptogram. The issuer then evaluates the transaction details.

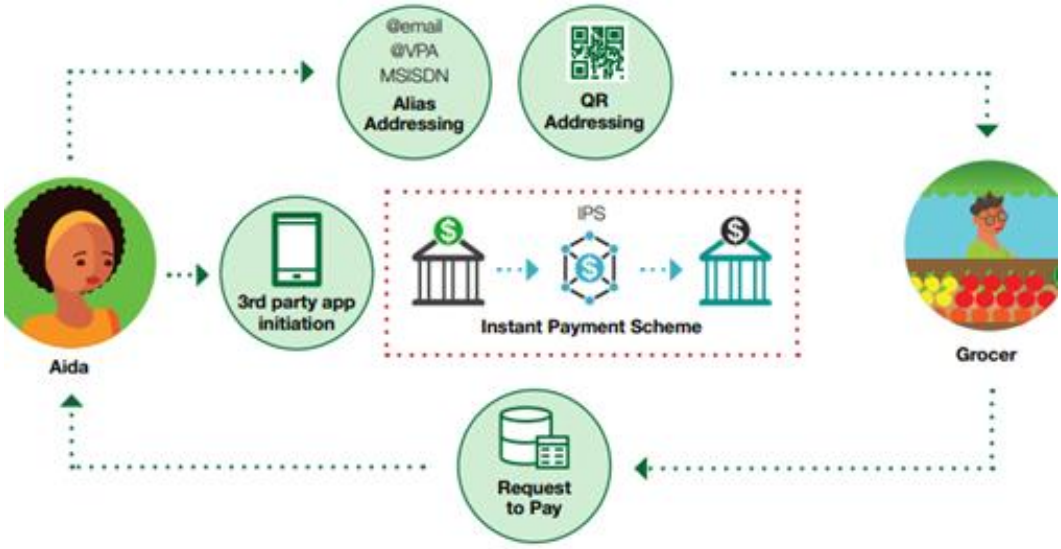

Figure 4: *Recent trends in payment initiation [5].*

Not all chip cards are identical; some are EMV cards, while others are chip and PIN cards. Both types utilize integrated circuit chips for enhanced security. The users have unique PIN for transaction verification. Key distinctions include that EMV technology serves as a global standard, while chip and PIN technology is primarily utilized in certain regions. Furthermore, chip and PIN cards are more frequently used for debit transactions, whereas EMV cards are generally associated with credit transactions. EMV technology has been in

existence since 1993 and has experienced significant adoption over the last 30 years. As depicted by **Figure 5**, "Worldwide, 88.55% of card-present transactions utilize the EMV chip. In Africa and the Middle East, this percentage rises to 98.69%, in Canada, Latin America, and the Caribbean, it stands at 95.34%, and in the United States, it is 84.84%" [6, p. 26]. EMV technology stores cardholders' data on an actual metallic chip which can only be read by specialized devices; thereby raising the security level.

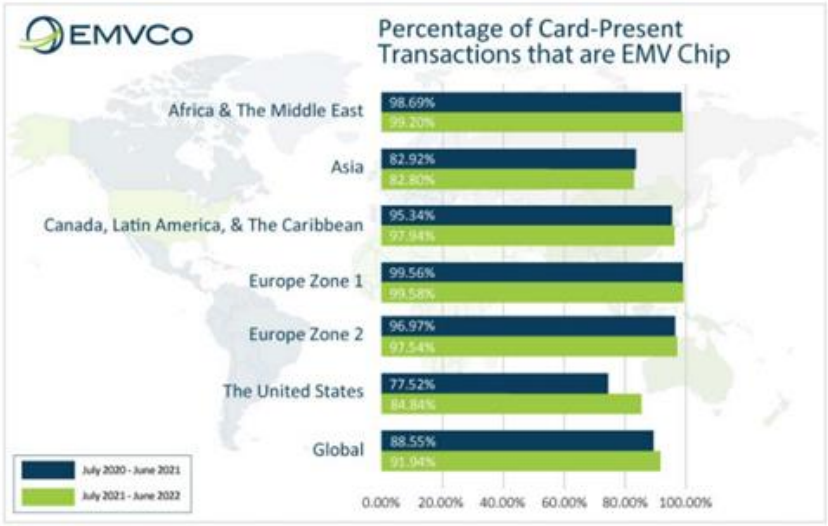

Figure 5: *EMV Transaction Percentage [6].*

4. Problem Statement

"Magnetic stripe cards, commonly known as magstripe or swipe cards, are the standard credit cards financial frequently use the magnetic stripe (often called magstripe) is a band of magnetic material containing iron-based particles capable of storing data" [6]. The stripe on the back is made up of modified iron-based magnetic particles that transfer data between the card and the terminal. These cards function as static storage devices, which the terminal reads during a swipe, subsequently handling PIN encryption and signature capture [11]. Here is how the process works: "When the card is swiped, the terminal sends an authorization request containing the customer's card data to the acquiring bank through some payment gateways. The acquiring bank then forwards this request to the issuing bank, such as Visa or Mastercard. The issuing bank responds with an authorization reply, which the acquiring bank relays back to the terminal" [11]. If all responses are approved, the transaction is completed. However, magstripe transactions are not individualized, meaning that stolen card information can be reused for future transactions.

In contrast, EMV chip cards feature a computer chip on the front **(Figure 6)** that communicates with terminals, allowing for a more secure and complex transaction process. EMV cards provide several advantages over magnetic stripe cards. First, upgrading to EMV is simple and cost-effective, with EMV-certified terminals available for around $200. Existing hardware can also be enhanced with custom integration. Second, EMV cards improve customer protection and foster trust. They ensure that each transaction is unique, which helps prevent duplicate or fraudulent charges. This reduction in fraud leads to fewer disputes and improved customer service.

Figure 6: *The front of a EMV card [6].*

5. Solution

EMV tags and EMV chips have provide a wide range of solutions for Fintech and Banking sectors. The first one is encryption technology. The payment information on old magnetic strip credit card was transferred in and out of banks in its original format. On the other hand, an EMV chip card codes this data into a format recognised by its bank software before transmitting it to the bank. This means that it is extraordinarily difficult for any person to intercept this kind of communication and decode the message passed between the card and the bank, thus protecting immensely from fraud. Due to this feature chip cards represent a much more secured way of payment, so users can feel safer as the confidential paying data is secured in the whole process. The second solution is improved card-to-bank communication.

Acquirer or issuers will get the EMV data as of list of (TLV) tags meaning Tag Length Value in BER-TLV (Basic Encoding Rules) format. This format is widely used in fintech as it is reliable way of transmitting the data between systems. These tags will provide the information about the card like card holder name, card number, expiration date, network and other details. **(Figure 7)** show more details about this TLV encoding.

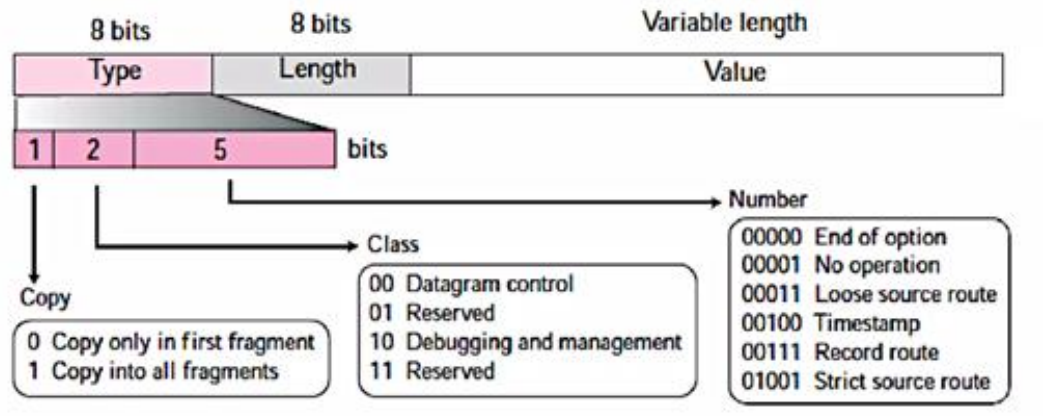

Figure 7: *TLV Encoding Explanation [7]*

Below is a sample EMV data in BER_TLV format and it also show how its decoded into

BER-TLV Format:

5A0C5234567890123456789 05F200E4D617279204A6F686E5F340211249F6E01029F1004234567899F26081 234567890ABCD9F3704000000029F360110

After Decoding:

5A0C52345678901234567890

Tag: 5A: Track 2 Equivalent Data (Card Number)

Length: 0C (12 bytes)

Data: 52 34 56 78 90 12 34 56 78 90 (Decoded:"5234567890123456")

5F200E4D617279204A6F686E

Tag: 5F20 - Cardholder Name

Length: 0E (14 bytes)

Data: 4D 61 72 79 20 4A 6F 68 6E

(Decoded: "Mary John")

5F34021124

Tag: 5F34 - Application Expiration Date

Length: 02

Data: 11 24

(Decoded: 11/24, meaning the card expires in November 2024)

9F6E0102

Tag: 9F6E - Card Network

Length: 01

Data: 02 (Assuming 02 indicates "MasterCard" or another specific network type)

There are many other tags like above which has specific meaning and purpose for each tag which help providing the information about the card and transaction.

An EMV card has a chip electric contact **(Figure 8)** requires the user to insert it into a slot on the reader, rather than swiping. Also, known as a dipping, this process does take a few seconds longer than a standard swipe. The chip uses these extra seconds to constantly send a stream of encrypted information back to the bank as proof that whoever is using this card is the card holder during said transaction. This may take some time to set up in the beginning, but the technology is most likely going to advance and speed up as banks and Fin-Tech continue serving customer in America and all over the globe. By having this counter started in the chip, it allows payments to be more secure and prevent fraudulent transactions, which adds higher security elements & builds trust in consumers.

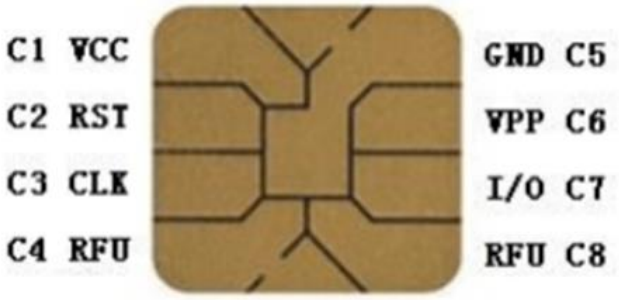

Figure 8: *Chip electric contacts [6].*

disappointed than swipe a magnetic stripe. No technology is 100% safe as far financial institutions should be concerned. Chip cards significantly cut down on fraud over magnetic stripe cards, but there is still other work to be done to safeguard the credit card and financial information of its customers.

6. Impact

Although it was first introduced by MasterCard more than 16 years ago, the U.S. did not begin the migration the chip-system until late 2016 [1]. Despite that, U.S. bank and more importantly, card issuers have now followed suit in adopting the EMV chip system, in the wake of various high-profile data breaches and escalating credit card fraud. This is an effort to secure customers' details and will also reduce the costs for fraud. Below is a list of the impacts of the EMV system.

Protection against fraud: The EMV chip is specifically intended to curb fraud. Magnetic strips **(Figure 9)** were created in the 1960s to facilitate transactions [8]. Then came EMV chips, which took things a step further by moving the innovation past convenience and over to security-arguing. Every other country that has implemented this technology for more than 10 years now reports drastically lower levels of in-person credit card fraud [1]. One of the reasons this remained unchanged for so long in America was a complex system providing rapid real-time internet service. In other words, the convenience of magnetic strips meant that banking and finance system would eventually get tired of dealing with the high rate of fraud.

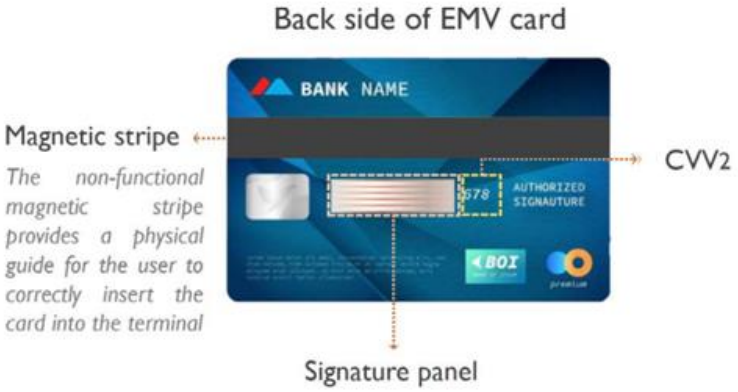

Figure 9: *The Magnetic strips [6].*

Unique Transaction Code: "When a chip card is used, it creates a unique transaction code which can only be used for that specific purchase and never duplicated" [8]. This is a very serious safety upgrade from the previous magnetic strip cards. Information is cloned easily with magnetic strip cards. In this case, once they have that information, they can use it over and over to make some unauthorized transactions. But thanks to EMV chip cards, users can no longer do that. Even if they get hold of the transaction data, it would be impossible for them to use this information to make fake purchases because the transfer code is not reusable — it has a unique identifier. If someone attempted to use the stolen info, the credit card charge would get denied. **Figure 10** depicts the additional functionalities of EMV. The introduction of EMV chip technology has therefore made targeting POS systems not only less profitable but also considerably an uphill challenge, especially for hackers and other unauthorized fraudsters.

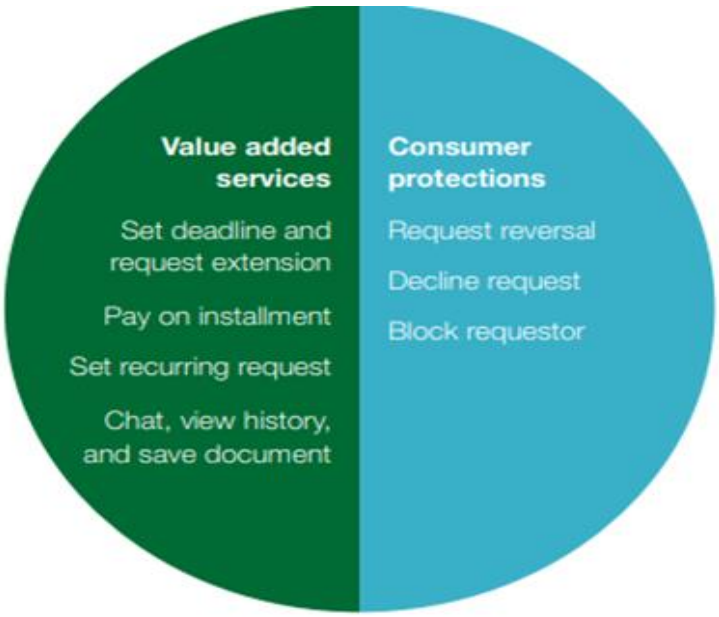

***Figure 10**: The additional functionalities of EMV [5].*

Nearly tamper proof: It is extremely difficult to tamper with a chip card. Inexpensive skimmers costing under $20 can be created by scammers to easily collect credit card details when a card is swiped at an ATM or gas pump [1]. On the other hand, the computer chips used in EMV-chip cards contain technology that is nearly counterfeit-proof. More recently, banks in the Unite States have introduced chips to its members' credit cards, meaning that it would take nearly a million dollars worth of equipment for scammers to get their hands on anything. The technology is too costly to be a practical investment for most scammers. In other words, the upfront fees need to tamper with chipped cards is too expensive for most fraudsters (and a much safer option when it comes to consumers). The EMV technology has played a key role in reading cards and securing transactions.

7. Uses

EMV has proven to be a crucial weapon in several banking and Fintech industries because it has a wide range of uses. This justified by the large number of worldwide EMV deployment **[Figure 11].** It helps prevent against physical world fraud. Experts agree that fraud in the physical world is already higher than the worldwide average and still increasing. Since fraud statistics are not documented as in other domestic markets, who knows exactly what the fraud rates are in the physical world, but anecdotal evidence from global migration activities is that fraud seems to migrate to areas that do not yet have EMV chip technology. Such nations include Malaysia and Thailand. With most of the world now either already on EMV (or planning to move to EMV), a country not adopting EMV could become a clear target for fraudsters, with fraud rates increasing, as the fraudsters move there. Transitioning to EMV would help avoid such challenges.

	2019		2020		2021	
Region	EMV Cards	Adoption Rate	EMV Cards	Adoption Rate	EMV Cards	Adoption Rate
Africa & the Middle East	312M	89.4%	339M	90.4%	375M	91.69%
Asia Pacific	6,226M	58.1%	6,885M	60.9%	7,528M	62.64%
Canada, Latin America, and the Carribbean	923M	86.7%	1,023M	90.7%	1,222M	90.56%
Europe Zone 1	1,040M	85.9%	1,073M	86.5%	1,192M	90.46%
Europe Zone 2	318M	80.7%	335M	84.1%	379M	86.29%
United States	1,074M	60.9%	1,161M	63.0%	1,282M	62.86%
Global	9,893M	63.8%	10,816M	66.4%	11,981M	68.16%

Figure 11: *Worldwide EMV deployment [6].*

EMV is used to foster payment transaction security. EMV improves transaction security in three ways. First, it provides card authentication. This helps prevent the use of counterfeit cards. In card-present situations, the chip makes use of an online card authentication between the emitter and the acquirer that checks for the presence of a valid account and can prevent counterfeit cards. If an online transaction is not possible, there are three other methods for offline use: "Static Data Authentication (SDA), Dynamic Data Authentication (DDA), and Combined DDA with application cryptogram generation (CDA)" [8]. EMC has precise data that renders any intercepted data unfit for transactions.

Second, "cardholder verification is the process of confirming the identity of the cardholder to prevent the misuse of lost or stolen cards". This step ensures the use us authorized. As depicted by **figure 12,** "The EMV protocol uses a chip and PIN system, where a small microprocessor chip is embedded in the card. When the card is used, the chip generates a unique code for each transaction" [6, p. 29]. The issuer determines which method to apply. Third, transaction authorization refers to the approval of transactions according to rules established by the issuer. The transaction details along with a unique cryptogram are sent to the issuer, who then either approves or declines the transaction, just like the process used with magnetic stripe cards in the U.S.

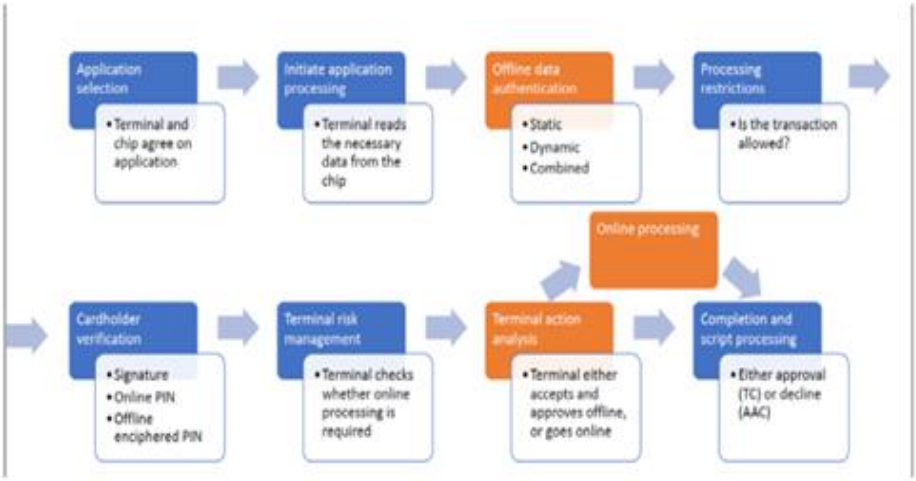

Figure 12: *Steps for EMV contact transaction [6].*

Data on EMV are more secure than information on magnetic stripe cards. The former uses "issuer-specific keys," which significantly enhances security. As a result, there has been an extensive global deployment of the technology **(Figure 13).** "For offline EMV transactions, the card and terminal rely on pre-set risk parameters to decide whether the transaction can go ahead. Offline transactions are particularly common in situations where terminals do not have online connectivity" [9] or where telecom costs are prohibitively high.

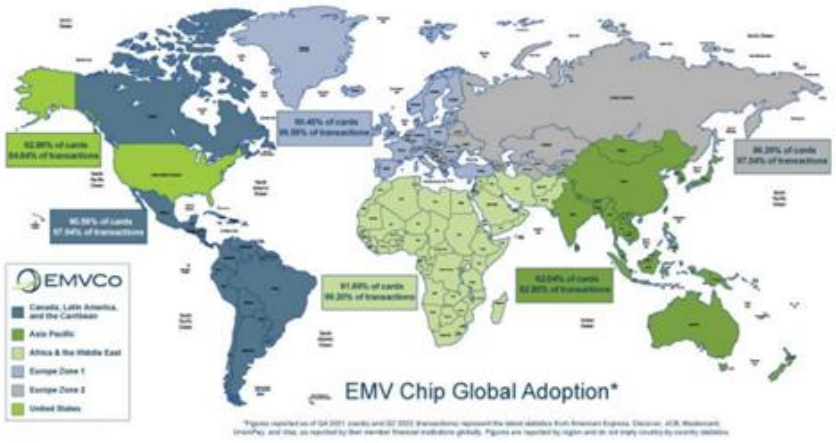

Figure 13: *EMV Deployment map [6].*

8. Conclusion

The implementation of EMV will change how terminals are deployed, managed, and how customers are onboarded. Despite of that, creating a business case for EMV is complex, but it's essential for all acquirers to begin building EMV capabilities. Acquirers should take lessons from the experiences of other markets while developing new tools to handle terminal software updates and reduce operational costs. It is important not to overlook the resources needed for EMV migration; establish timelines for implementation and keep an eye on resource limitations. Careful planning is vital, meaning companies should start preparing for the future now. Postponing EMV migration raises risks for both the business and its customers. While the EMV Chip Specifications help reduce fraud risk, they do little to protect against card-not present transactions. Besides, the speed at which e-commerce and online shopping has grown really exposes this as the big weakness that security experts expect to be targeted as the focus of credit card fraud moving forward. As a result, the EMV Specifications have developed from the original EMV chip to improvements such as the EMV 3-D Secure. It is easy for users, especially hackers to read the information on conventional magnetic stripes. On the other hand, EMV technology stores cardholders' data on an actual metallic chip which can only be read by specialized devices; thereby raising the security level.

References

[1]. D. Basin, R. Sasse, and J. Toro-Pozo, "The EMV Standard: Break, Fix, Verify," IEEE Xplore, May, 01, 2021. https://ieeexplore.ieee.org/abstract/document/9519404

[2]. M. A. Ali, M. A. Azad, M. Parreno Centeno, F. Hao, and A. van Moorsel, "Consumer-facing technology fraud: Economics, attack methods and potential solutions," Future Generation Computer Systems, vol. 100, no. 1, pp. 408–427, November, 2, 2019. https://doi.org/10.1016/j.future.2019.03.041.

[3]. W. Ahmed et al., "Security in Next Generation Mobile Payment Systems: A Comprehensive Survey," IEEE Access, vol. 9, pp. 115932–115950, 2021, doi: https://doi.org/10.1109/access.2021.3105450.

[4]. OECD, The FinTech Ecosystem in the Czech Republic. OECD Publishing, November, 15, 2022. https://www.oecd.org/en/publications/the-fintech-ecosystem-in-the-czech-republic_068ba90e-en.html

[5]. W. Cook, D. Lennox & S. Sbeih. "Starting the transaction: payment initiation and customer experience," April, 2023. https://www.cgap.org/sites/default/files/publications/Starting%20the%20Transaction-compressed.pdf

[6]. Ayooluwa Olosunde Understanding EMV, Introduction to TLV, April, 09, 2023. https://medium.com/@lovisgod/understanding-emv-introduction-to-tlv-40d66bd004e7

[7]. I. Dubinsky, Cryptography for Payment Professionals. CRC Press, May, 10, 2023. https://www.routledge.com/Cryptography-for-Payment-

Professionals/Dubinsky/p/book/9781032442747?srsltid=AfmBOorulL4Tp4WMVMf-eT75wcRkIldctNnIoB_l69qFuTxCfvPvBtV2

[8]. J.-N. Luo and M.-H. Yang, "EMV-Compatible Offline Mobile Payment Protocol with Mutual Authentication," Sensors, vol. 19, no. 21, p. 4611, Oct. 2019, https://doi.org/10.3390/s19214611.

[9]. E. Brumercikova and Bibiana Bukova, "Proposals for Using the NFC Technology in Regional Passenger Transport in the Slovak Republic," Open Engineering, vol. 10, no. 1, pp. 238–244, March, 2020, doi: https://doi.org/10.1515/eng-2020-0005.

[10]. D. Basin, C. Cremers, J. Dreier, and R. Sasse, "Tamarin: Verification of Large-Scale, Real-World, Cryptographic Protocols," IEEE Security & Privacy, pp. 24–32, February, 16, 2022, https://doi.org/10.1109/msec.2022.3154689.