EMV Chip and PIN: A Feeble Upgrade

Naga Suraj Maddi
nsmaddi@stcloudstate.edu

Follow this and additional works at: https://repository.stcloudstate.edu/msia_etds

Recommended Citation
https://repository.stcloudstate.edu/msia_etds/76

This Starred Paper is brought to you for free and open access by the Department of Information Systems at theRepository at St. Cloud State. It has been accepted for inclusion in Culminating Projects in Information Assurance by an authorized administrator of theRepository at St. Cloud State. For more information, please contact rswexelbaum@stcloudstate.edu.
EMV Chip and Pin: A Feeble Upgrade

by

Naga Suraj Maddi

A Starred Paper
Submitted to the Graduate Faculty of
St. Cloud State University
in Partial Fulfillment of the Requirements
for the Degree
Master of Science in
Information Assurance

December, 2018

Starred Paper Committee:
Susantha Herath, Chairperson
Lynn Collen
Balasubramanian Kasi
Abstract

The most dominant protocol used in the smart card payments all over the world is called EMV (EMV, n.d.) which stands for Europay, MasterCard and Visa. The EMV cards are used for processing transactions through payment terminals and ATMs (automated teller machine). These are widely used in Canada, Mexico, Europe, Asia, South America and was also implemented in USA (Huq, 2015). The transactions of the EMV are secured by using a variety of cryptographic authentication codes, digital signatures and an entry of a PIN. But in US there was a slightly different implementation which led to a disaster as they ended up less secure, slow and confusing to use. This paper will discuss about the problems and challenges faced in USA due to this implementation and focus on flaws in the protocol. Identify different ways in which the transactions were compromised and study the statistics to get a brief idea about the types of compromises occurring frequently. This paper also discusses about future of making secure transactions and alternate ways to achieve it. It will also include a survey aimed to identify whether EMV has been implemented successfully and if chip cards are being used and to which extent. Other sources of payment are also focused to find where the interest must be shifted for research in secure future payment systems.
# Table of Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. Introduction</td>
<td>8</td>
</tr>
<tr>
<td>Introduction</td>
<td>8</td>
</tr>
<tr>
<td>Problem Statement</td>
<td>9</td>
</tr>
<tr>
<td>Nature and Significance of the Problem</td>
<td>10</td>
</tr>
<tr>
<td>Objective of the Research</td>
<td>10</td>
</tr>
<tr>
<td>Research Questions</td>
<td>10</td>
</tr>
<tr>
<td>Limitations of the Research</td>
<td>11</td>
</tr>
<tr>
<td>Definition of Terms</td>
<td>12</td>
</tr>
<tr>
<td>Summary</td>
<td>13</td>
</tr>
<tr>
<td>II. Background and Review of Literature</td>
<td>14</td>
</tr>
<tr>
<td>Introduction</td>
<td>14</td>
</tr>
<tr>
<td>Background Related to the Problem</td>
<td>14</td>
</tr>
<tr>
<td>Literature Related to the Problem</td>
<td>19</td>
</tr>
<tr>
<td>Literature Related to the Methodology</td>
<td>38</td>
</tr>
<tr>
<td>Summary</td>
<td>46</td>
</tr>
<tr>
<td>III. Methodology</td>
<td>48</td>
</tr>
<tr>
<td>Introduction</td>
<td>48</td>
</tr>
<tr>
<td>Chapter</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Design of the Study</td>
<td>48</td>
</tr>
<tr>
<td>Data Collection</td>
<td>49</td>
</tr>
<tr>
<td>Tools and Techniques</td>
<td>49</td>
</tr>
<tr>
<td>Summary</td>
<td>50</td>
</tr>
<tr>
<td>IV. Data Presentation and Analysis</td>
<td>51</td>
</tr>
<tr>
<td>Introduction</td>
<td>51</td>
</tr>
<tr>
<td>Data Presentation</td>
<td>51</td>
</tr>
<tr>
<td>Data Analysis</td>
<td>54</td>
</tr>
<tr>
<td>Summary</td>
<td>71</td>
</tr>
<tr>
<td>V. Results, Conclusion, and Recommendations</td>
<td>73</td>
</tr>
<tr>
<td>Introduction</td>
<td>73</td>
</tr>
<tr>
<td>Results</td>
<td>73</td>
</tr>
<tr>
<td>Conclusions</td>
<td>88</td>
</tr>
<tr>
<td>Future Works</td>
<td>90</td>
</tr>
<tr>
<td>References</td>
<td>92</td>
</tr>
<tr>
<td>Appendix</td>
<td>96</td>
</tr>
</tbody>
</table>
# List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Definition of Terms</td>
<td>12</td>
</tr>
<tr>
<td>2. Attack Tree Node Mapping</td>
<td>35</td>
</tr>
</tbody>
</table>
## List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>SMB confidence to meet EMV deadline</td>
<td>16</td>
</tr>
<tr>
<td>2.</td>
<td>Log data submitted by bank</td>
<td>20</td>
</tr>
<tr>
<td>3.</td>
<td>Attack tree modeling at POS</td>
<td>37</td>
</tr>
<tr>
<td>4.</td>
<td>Fraud levels on the payment cards</td>
<td>39</td>
</tr>
<tr>
<td>5.</td>
<td>Company categories</td>
<td>43</td>
</tr>
<tr>
<td>6.</td>
<td>Payment security technology plans</td>
<td>44</td>
</tr>
<tr>
<td>7.</td>
<td>Alternative payment types</td>
<td>46</td>
</tr>
<tr>
<td>8.</td>
<td>Survey responses of 1 – 50 participants</td>
<td>53</td>
</tr>
<tr>
<td>9.</td>
<td>Survey responses of 51 – 100 participants</td>
<td>54</td>
</tr>
<tr>
<td>10.</td>
<td>Survey report Q1</td>
<td>55</td>
</tr>
<tr>
<td>11.</td>
<td>Survey report Q2</td>
<td>55</td>
</tr>
<tr>
<td>12.</td>
<td>Survey report Q3</td>
<td>56</td>
</tr>
<tr>
<td>13.</td>
<td>Survey report Q4</td>
<td>57</td>
</tr>
<tr>
<td>14.</td>
<td>Survey report Q5</td>
<td>58</td>
</tr>
<tr>
<td>15.</td>
<td>Survey report Q6</td>
<td>59</td>
</tr>
<tr>
<td>16.</td>
<td>Survey report Q7</td>
<td>60</td>
</tr>
<tr>
<td>17.</td>
<td>Survey report Q8</td>
<td>62</td>
</tr>
<tr>
<td>18.</td>
<td>Survey report Q9</td>
<td>64</td>
</tr>
<tr>
<td>19.</td>
<td>Survey report Q10</td>
<td>65</td>
</tr>
<tr>
<td>20.</td>
<td>Survey report Q11</td>
<td>66</td>
</tr>
<tr>
<td>Figure</td>
<td>Survey report Q12</td>
<td>Page</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------</td>
<td>------</td>
</tr>
<tr>
<td>21.</td>
<td>.................................</td>
<td>67</td>
</tr>
<tr>
<td>22.</td>
<td>.................................</td>
<td>68</td>
</tr>
<tr>
<td>23.</td>
<td>.................................</td>
<td>69</td>
</tr>
<tr>
<td>24.</td>
<td>.................................</td>
<td>70</td>
</tr>
<tr>
<td>25.</td>
<td>.................................</td>
<td>74</td>
</tr>
<tr>
<td>26.</td>
<td>.................................</td>
<td>74</td>
</tr>
<tr>
<td>27.</td>
<td>.................................</td>
<td>76</td>
</tr>
<tr>
<td>28.</td>
<td>.................................</td>
<td>76</td>
</tr>
<tr>
<td>29.</td>
<td>.................................</td>
<td>78</td>
</tr>
<tr>
<td>30.</td>
<td>.................................</td>
<td>78</td>
</tr>
<tr>
<td>31.</td>
<td>.................................</td>
<td>80</td>
</tr>
<tr>
<td>32.</td>
<td>.................................</td>
<td>80</td>
</tr>
<tr>
<td>33.</td>
<td>.................................</td>
<td>82</td>
</tr>
<tr>
<td>34.</td>
<td>.................................</td>
<td>82</td>
</tr>
<tr>
<td>35.</td>
<td>.................................</td>
<td>84</td>
</tr>
<tr>
<td>36.</td>
<td>.................................</td>
<td>85</td>
</tr>
<tr>
<td>37.</td>
<td>.................................</td>
<td>87</td>
</tr>
</tbody>
</table>
Chapter I: Introduction

Introduction

Smart cards have replaced the use of magnetic stripe cards for point-of-sale and Automated Teller Machine transactions in many countries which include U.S.A, Canada, Mexico, Europe, Asia, and South America. EMV stands for Europay, MasterCard and Visa which are the three companies who had created the standard (EMV, n.d.). EMV is the new technical standard for performing transactions with the smart cards by using devices which accept them. The EMVCo now manages the standard, a consortium, with control equally divided between MasterCard, Visa, JCB, American Express, Discover and China UnionPay. The EMV consortium was created in 1994 for developing new technologies that counteract to card payment fraud. EMV features a chip in the cards that store cryptogram which allow banks to determine if the transaction or card has been altered. The chip in the cards also has a counter which increments on each transaction to avoid duplication of counter values which indicate possible fraudulent activities.

In EMV, the customer authenticates a transaction by using their smart card (credit/debit card) which is inserted into a Point of Sale terminal (POS) and a PIN is entered in it. Then the PIN is verified by the ICC (Integrated Circuit Chip) and is authenticated to the terminal using DS (digital signature) (Murdoch, Drimer, Anderson, & Bond, 2010). The details of the transaction are also verified using a cryptographic Message Authentication Code (MAC), with the use of a symmetric key shared between the card used for the payment and the bank which issued the card. Though it was
expected to be a very secure payment system, it was hacked several times, and the protocol which was meant to be secure became weak. The use of payment cards is widespread in the day to day life, and it should be a robust and secure system to rely on. There is a need to identify more secure ways to do day to day transactions and should be easy and comfortable for the users of the transaction system.

**Problem Statement**

The implementation of the EMV was not very successful. In the USA, the transition to chip cards had been a very big disaster (Kar, 2016). The implementation led to a confusing, very slow and less secure payment option than the alternative payment modes. There are two types of cards called Chip-and-pin cards and Chip-and-signature cards based on the methods of authentication enforced by the issuer of the card. There was a slightly different implementation in the USA than other countries where the governments established as a mandate to upgrade the systems by a specific date. The U.S. implemented the "Liability Shift" which was a significant wrong step for its failure. One more specific reason it failed was that the USA had opted for Chip-and-signature cards so that the banks do not want to put a burden on the customers to remember a 4-digit code at the checkout (Next-gen, 2015). These were few of the significant steps for the failure in USA. This study helps in analyzing the weakness of the system and ways to prevent it if it can be achievable. This study will also guide for other payment modes providing a quick and more secure means.
Nature and Significance of the Problem

The use of EMV smart cards is embedded into our daily life. This system which is used massively must be something on which one can rely on. But this trust had been broken as many compromises that occur in the system are witnessed which weakens the faith in such a widely-used system. So, this study is an effort to analyze the issues of the EMV standard whether the system can still be made robust by making any possible fixes. Is there any better solutions rather than relying on the EMV and the ways to secure ourselves to build the future of payment methods more secure and easy to use.

Objective of the Research

The objective of this study is to understand the working of the EMV standard which is used for making secure transactions using smart cards and to find possible fixes to make this system more robust and secure. This study also focuses on the next steps to the EMV smart cards and ways to achieve safe and fast transactions in the future in an effective manner.

Research Questions

1) What are EMV cards, are people aware about them and do individuals possess the new EMV cards?

2) What are the modes of payment used by individuals for their day to day transactions and their frequent mode of payment?

3) What type of authentication is preferred while performing card transactions by the individuals?
4) Do individuals prefer smart cards over magnetic stripe cards and how secure do they feel about using them?

5) What are the modes of payments used by retailers and had the EMV chip card equipment is installed in major retail stores?

6) Did attacks reduce after shifting to EMV and are people affected even after the shift to EMV cards?

7) What is the best alternative to EMV cards and are people using it?

8) What method of shopping consumers prefer using to identify the areas towards which focus needs to be increased?

**Limitations of the Research**

This research tries to answer the study questions based on the information collected through survey. Hence, in terms of real world, the results may deviate as the results are more inclined towards the survey population but tries to best answer the study questions under this research’s limitations. Some questions have been cross verified like the survey questions Q5 and Q7 which ask about the EMV cards but a slight difference in the responses are observed showing that the data is not 100% accurate.
**Definition of Terms**

Table 1

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMV</td>
<td>Europay, MasterCard and Visa which is a standard</td>
</tr>
<tr>
<td>ATM</td>
<td>Automated Teller Machine</td>
</tr>
<tr>
<td>POS</td>
<td>Point of Sale</td>
</tr>
<tr>
<td>ICC</td>
<td>Integrated Circuit Chip</td>
</tr>
<tr>
<td>DS</td>
<td>Digital Signature</td>
</tr>
<tr>
<td>2FA</td>
<td>2 Factor Authentication</td>
</tr>
<tr>
<td>PCB</td>
<td>Printed Circuit Board</td>
</tr>
<tr>
<td>ATR</td>
<td>Answer to Reset</td>
</tr>
<tr>
<td>FPGA</td>
<td>Field Programmable gate array</td>
</tr>
<tr>
<td>LOC</td>
<td>Line of Code</td>
</tr>
<tr>
<td>iCVV</td>
<td>Card verification value for integrated circuit boards</td>
</tr>
<tr>
<td>UN</td>
<td>Unpredictable number</td>
</tr>
<tr>
<td>ATC</td>
<td>Application Transaction Counter</td>
</tr>
<tr>
<td>NFC</td>
<td>Near Field Communication</td>
</tr>
<tr>
<td>HCE</td>
<td>Host-card Emulation mode</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>CVV</td>
<td>Card Verification Value</td>
</tr>
<tr>
<td>UI</td>
<td>User Interface</td>
</tr>
</tbody>
</table>
Summary

This chapter focused on the current trend of the standards being used for making transactions in our day to day life. It covers about the smart cards which have a chip and are inserted followed by the entry of a pin for performing secure transactions (Murdoch et al., 2010). The implementation of the EMV standard in different countries have been identified and explains the reasons for the failure of transition in the USA (Next-gen, 2015). It contains the objectives of the study related to the problems of current system and identify alternatives to make the future of transactions safe and comfortable to use followed by questions for the researchers to focus on and briefed the list of terms that would be used in the paper. The next chapter focuses on the background of the problem, whether any research has been done on the situation and what methodologies have been used to tackle the problem.
Chapter II: Background and Review of Literature

Introduction

The implementation of EMV cards had replaced the traditional magnetic stripe with the use of embedded microprocessors which store the data of the cardholder. This implementation had boosted the payment card security though it has its share of the security challenges of its own. By using the PIN-based authentication option, it could cut down the fraud which involved the lost and stolen cards. It had also addressed counterfeit fraud which could lead to data breaches but not completely (Next-gen, 2015). It provided better protection for this fraud than what the traditional cards would handle.

Though EMV was secure but considering the recent attacks which took place exposed its weaknesses, and it is now in a position where one cannot trust these cards for its reliability. The implementation of this transition in the US had been a failure because of the scheme used for its implementation (Kar, 2016). This chapter focuses on the background, research that has been done on the problem and how it relates to this paper. Then it describes the methodology that will be used in the study followed by the summary of this chapter.

Background Related to the Problem

Before the introduction of the Chip and Pin cards, magnetic stripe cards were used for the credit/ debit card transactions where the data was read and recorded about the account followed by a signature for authentication. After the card is swiped at the terminal, a receipt is printed once the account details are verified by the system, and the
customer had to sign the receipt and return it to the clerk who operates the swiping machine. Then the clerk had to verify the signature on the receipt if it matches the signature on the back of the card to authorize the transaction (EMV, n.d.). But this system had numerous security flaws with the possibility that the card could be stolen and that the signature could be forged to perform the transactions. But as the technology advanced, there was even equipment available in the black markets where data could be read and written to the magnetic stripes which makes it easier to clone the original cards and use them without the knowledge of the card owner (EMV, n.d.). With all these events the EMV was introduced which could tackle with such issues and provide security for the card transactions.

The switch to EMV cards had not been very successful in the case of U.S.A. EMV stands for Europay, MasterCard and Visa was launched in 1994 as a standard to bring a change in the security of payment cards. EMV uses smart cards which have Integrated Circuits which hold the information of the card reader. This implementation even needed hardware devices which accept the EMV cards for performing the transactions. This was a huge step as it involved lots of expenditure and the whole system had to be upgraded. EMV was implemented in many countries which include Africa, Asian/Pacific countries, Europe, North America, Latin America, and the Caribbean. The implementation of the upgrade in the U.S. was different from other countries. The governments of other countries established by mandating a specific date by which the systems had to be upgraded. In the U.S., the government introduced "liability shift" which meant that if the retailers did not support the chip card payments by
not upgrading their systems with the new and expensive machine, then they would be held responsible for any fraud that occurs in the store. In general, it is the responsibility of the bank (Kar, 2016). So, it summarized that if the retailers purchased the new card reading terminals, then the liability would shift back to the bank otherwise the retailer will be held responsible for the fraud that occurred in their store.

The process of upgrading the systems was also very slow. Even in October 2015, many U.S. retailers were not ready with the new EMV standard. Only 22% of the midsize retailers were ready for the EMV deadline. The number of retailers that are EMV complaint is trending in a positive direction as it doubled from 11% to 22% from 2014 to 2015.

Below is a pie chart showing the midsize businesses confidence for meeting the EMV deadline.

<table>
<thead>
<tr>
<th>Confidence Level</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not at all confident</td>
<td>9%</td>
</tr>
<tr>
<td>Minimally confident</td>
<td>17%</td>
</tr>
<tr>
<td>Moderately confident</td>
<td>22%</td>
</tr>
<tr>
<td>Very confident</td>
<td>11%</td>
</tr>
<tr>
<td>Extremely confident</td>
<td>13%</td>
</tr>
<tr>
<td>Already have EMV terminals</td>
<td>22%</td>
</tr>
<tr>
<td>Unaware of deadline</td>
<td>7%</td>
</tr>
</tbody>
</table>

N = 252
Though it showed a positive trend, 78% of the retailers were still not EMV-compliant (Guinn, 2015). If the shops received the new equipment to accept chip cards did not mean to start accepting the chip cards immediately. There were payment processors who had to certify that their systems were still compatible and worked correctly before turning on the chip readers. This process took several weeks to start their terminals which ran beyond the scheduled time.

The introduction of liability shift was to give support to the retailers for upgrading their systems without forcing them. Many big retailers like WalMart and Target were losing millions of dollars in fraud due to the use of magnetic stripe cards and introducing the liability shift was a benefit to them. But smaller stores like coffee shops, bars did not consider the fraud as a very big deal and they felt the liability shift less of an incentive as they had to spend tens of thousands of dollars for replacing the equipment and it was the main reason for small business owners not supporting the chip cards (Kar, 2016).

One more significant false step that banks implemented was to opt for Chip and signature cards which created a less secure payment system. The banks chose the signature vs. PIN code as it saved a huge amount of money by avoiding the need to store the PIN codes for everyone. On the other hand, banks said that customers would have difficulty remembering a 4-digit code. But millions of people were already using check cards and other types of cards which required PIN codes. Hence the simple fact was that banks opted a less secure way while a much secure version was available.
An important point to be considered is that just by replacing a dumb card with a smart card will not help in solving the problem of knowing the identity of the cardholder. The EMV needs an identity authentication to get a complete solution for stopping fraud. People do not observe skimming attacks as a sound attack on the user’s true identity. Hence, they will keep using the EMV cards which they think is a smarter version of the dumb version (The dumb, 2016). The hackers will continue to steal data continuously as the banks, and card issuers sell these cards saying that the cards are not skimmable and make implications of a person’s true identity. One fact which should be kept in mind is that the fraud keeps flowing to the places where there are weaknesses. As the people around the world keep using these smart cards, the hackers keep collecting the EMV track 2 data for creating fake cards and use them on the ATMs which have not yet upgraded to accept EMV cards and perform transactions using chip and PIN. A large-scale fraud had occurred in Japan in recent years with the use of international cards, and the fraud had also flown to Brazil. In these areas, a biometric system was used for identifying the user identity. A card plus fingerprint solution was implemented by the banks and ATMs, but the hackers still could make a way out and used the replication cards in ATMs which were still not upgraded with the new solution thus resulted in a fraud (The dumb, 2016).

This paper is an effort to identify the problems about the failure in a detailed manner and to find alternatives to find more secure payment options.
Literature Related to the Problem

EMV is a standard which was introduced for performing transactions using smart cards. It required a specialized hardware and software upgrade to implement this standard for conducting secure transactions. EMV can be called as a chip-based payment card system. The chip inside it creates a dynamic and unique code for every transaction which significantly reduces the risk of counterfeit attacks as the Point-of-sale (POS) systems (Conroy, 2014). In the U.S., credit card fraud rates doubled from five basis points to 10 basis points from 2007 through 2014. There was a rapid increase rate of debit card fraud due to the attacks like skimming techniques to track the data of the card and the PIN of the cardholder.

The EMV cards were believed to be very resistant against frauds. But this particular case related to EMV cards exposed a flaw. Mr. Gambin is a customer of HSBC who was a Maltese customer was refused by the bank a refund about the series of transactions which were billed to his card account which the bank claimed that he had used his card and PIN at an Automated Teller Machine (ATM) in Palma, Majorca on June 29, 2011. In such cases, the victim of the fraud is suggested to demand logs of the transaction from the bank. In most the cases the banks either refuse to furnish them or may even delete the logs during the dispute leaving the customer to argue about the generalities. Some courts have criticized the banks recently, and in the case of Gambin, the bank produced a detailed log record. It was found that one of the fields of the log file which is the Unpredictable number also called as UN was found to be increasing steadily. The log data which was submitted by the bank is shown in the below picture.
The Unpredictable number was found to have a 17-bit fixed value, and the low 15 bits were simply a counter which is incremented every few milliseconds which was cycling every three minutes. This brought up the fact that the Unpredictable number which is generated at the ATMs could be predictable. This could create an opportunity for a hacker who has temporary access to a card could compute the authentication codes which are required to withdraw cash from an ATM at some time in the future at which the UN number could be predicted. This type of scenario is called a pre-play attack. After analysis on few more ATMs, they discovered that ATMs generated a poor random number and this strategy could be used to perform such attacks (Bond et al., 2014).

From November 27, 2013, to December 15, 2013, there was a data breach in Target which exposed personal information, credit/debit card numbers, names, mailing addresses and phone numbers of 40 million customers to fraud. The Point-of-sale systems were compromised which exposed the security PINs of millions of payment cards. At that time, there were less than 1 percent of cards which used the EMV technology for payment where as 80 other countries were already using the EMV

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>UN</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011-06-29</td>
<td>10:37:24</td>
<td>F1246E04</td>
</tr>
<tr>
<td>2011-06-29</td>
<td>10:37:59</td>
<td>F1241354</td>
</tr>
<tr>
<td>2011-06-29</td>
<td>10:38:34</td>
<td>F1244328</td>
</tr>
<tr>
<td>2011-06-29</td>
<td>10:39:08</td>
<td>F1247348</td>
</tr>
</tbody>
</table>

Figure 2: Log data submitted by bank (Reprinted from Bond, Choudary, Murcoch, Skorobogatov, & Anderson, 2014).
systems. This was the scenario when the hackers took the advantage of America’s reliance on magnetic stripe cards which was an outdated system that offered less protection against the new and advanced threats. After this incident was released to public the card issuers made a statement to upgrade to the EMV systems (Next-gen, 2015). The other factors include the difficulty of using magnetic stripe cards at overseas, the decrease in the cost of terminals and the chips lead U.S. to take a decision to upgrade their payment infrastructure and adopt the EMV standards.

The strategy of U.S. to implement this upgrade was different from other countries which mandate to upgrade the systems by a fixed date. U.S. implemented liability shift which was scheduled on October 1, 2015 (Kar, 2016). The retailers had to buy the expensive machines which accept the chip cards. The retailers who do not prefer to upgrade will be liable if any fraud occurred in their store. Otherwise the liability will be shifted back to the bank which issued the card. This shift was called as a liability shift. Big retailers like Walmart had huge loss of money due to the swiping card mechanism and they felt this shift as an incentive to reduce the fraud which occurred in their stores. But small retailers like Starbucks were not affected much due to the fraud and they felt the incentive as a burden as they had to spend tens of thousands of dollars to buy the equipment. On October 1, 2016, a new liability shift occurred where the Automated Teller Machines (ATMs) which accept Mastercard branded cards must be EMV operational and the machines which accepted VISA branded cards have another year to be operational (Figliola, 2016).
The next major issue which was highlighted was regarding the adoption of Chip and Signature mechanism which was not very secure while a more secure option of Chip and PIN was available. The critics raised that the banks wanted to save the extra expenditure that would incur to store the PIN numbers of every individual. While the banks stated that they did not want their customers to have a burden of storing a 4-digit PIN to perform transactions (Kar, 2016). Due to this implementation, the EMV cards does not stop Lost and stolen cards fraud as they can be used to perform transactions by forging the signature (Figliola, 2016).

The EMV cards used 2 factor authentication (2FA) as it required the chip to be inserted into the reader followed by the entry of a PIN by user to authenticate a transaction making it secure. Even with such secure implementation, a fraud took place where a group of criminals used a new trick to outsmart the chip and pin technology few years ago. According to wired (Greenberg, 2015), in 2011 and 2012 five French citizens were arrested for doing fraudulent transactions on stolen credit cards. They used 40 separate cards and made 7000 transactions and made purchases worth $680,000 USD. After the criminals were caught, a forensic investigation was conducted and was determined that they used a “man in the middle” attack which compromised the communication channels which were used by the cards and card readers by implanting a second chip inside every stolen card. The forged module was different in appearance as it was engraved with the inscription ‘FUN’ and there were traces of glue which clearly show that a foreign module replaced the original chip of the card. Further investigation revealed that it had connection of wires made with gold between the FUN card module
and the stolen copper chip. This made the card slightly bulging but could fit into a POS system. The forged module effect takes place during the verification of the card holder and transaction authorization processing. When the POS asks for user’s PIN, the FUN card replies to the POS machine that any PIN entered is correct and when the transaction authorization step is being performed, FUN card relays the transaction data between the POS system and original chip used by the reader to accept the purchase. EMVCo is the consortium which manages the EMV standard reported that they patched the vulnerabilities when the criminals were arrested (Bisson, 2015). But the researchers declined to fully detail the new security measures (Jain, 2015).

Even after the implementation of the payment network’s “Liability shift” which puts the burden over the merchants for fraud if they did not use EMV accepting POS systems which failed. As a result, customers always face confusion and are delayed at the checkouts for making payments. Many small and mid-size retailers which are independent still rely on magnetic strip cards which are insecure despite they received a warning from the banks and card issuing companies that the cards which would be used may expose to fraud and the data collected by hackers through skimming can be used by hackers to buy goods in unauthorized manner.

Numerous types of attacks were possible on the EMV cards whose standard was felt to be very secure and mitigate fraud. Man-in-the-middle Attack, Pre-Play Attack, NFC Relay Attack, Shim-in-the-middle Attack and various kinds of Eavesdrop attacks are some attacks to name a few.
An important weakness of the EMV protocol is in the PIN (Personal Identification Number) verification step where it was never clearly authenticated (Murdoch et al., 2010). A device which is designed to perform man-in-the-middle can successfully accomplish the attack if it can intercept and make modifications to the communication between the POS terminal and the card. In this attack, it makes the terminal believe that PIN verification has been done and it is successful while it tells the card that the PIN verification was not attempted and a different mechanism was used like signature for verification. The fake PIN which was entered never reaches the card thus the PIN retry counter on the card is unaltered.

Skimming was another kind of attack in which the information on the magnetic stripe of the card was forged. This attack was shown as a practical exhibition and explained how the attack is performed by Josef Langer and Michael Roland. PPA which stands for Pre-play attack was used to extract dynamic card verification codes also called as CVC which were needed for the authorization of the payment. They had also showcased a weakness of the credit cards by downgrading the CVM mode to the traditional magnetic stripe mode. Another kind of PPA was also demonstrated where the unpredictable number (UN) for the Automated teller machines (ATM) was predicted. But in this attack, the target is limited to contactless EMV protocol in the magnetic stripe mode. The maximum limit in the attack is the highest amount of money that can be authorized on a contactless card transaction (Vila & Rodriguez, 2015). The contactless EMV payment systems have four (1, 2, 3, 4) kernel specifications. This attack scenario uses Kernel 2 specifications for interaction with the payment cards supporting
MasterCard pay Pass or similar cards. In Kernel 2 specification, the Unpredictable number (UN) is a 4-byte value which is limited by a BCD-encoding numeric value that ranges from 0 - 99,999,999 and if the method was downgraded to the magnetic stripe protocol, the UN was reduced to 0 - 999. This specific set of UN could be predicted in about a minute using an android app running on a google galaxy nexus S (Vila & Rodriguez, 2015). The information required for a successful payment transaction can be generated if the attacker can communicate for a minute with the EMV magnetic stripe card. The UN, card secret key and the application transaction counter are used to get the CVC. EMV tackles replay attacks by increasing the Application transaction counter (ATC). An attacker can only use single ATC + CVC set per single transaction. The hacker clears the flag containing the EMV mode by overwriting AIP thus downgrading it to the magnetic stripe method. The magnetic stripe mode data which is returned in GET PROCESSINGOPTIONS is not authenticated. With the help of this data hacker can create a functional contactless clone with the pre-played data. To showcase a successful combined pre-play attack and downgrade to a magnetic stripe attack scenario, the attacker needs a system involving a JAVA card application and an Android app. The Galaxy Nexus running the Android app collects the magnetic stripe data and the pre-play data from a genuine card from its contactless interface which can later be transferred to a Java card using the same application.

An easy fix for this type of attack is by using a cryptographically secure random number generator for generating the UN. The card holder can also prevent this attack
by keeping the card in a box which is made of aluminum. Banks can stop this attack by digitally signing the CVM list so that the attacker cannot alter the list.

NFC relay attacks are another type of attacks which could be performed on the EMV cards. Ricardo J. Rodriguez and Jose Vila displayed alternative implementations of the attack using mobile devices which were NFC enabled (Kfir & Wool, 2005). This attack is a passive relay attack. It works in such a way that the hacker will trick the payment system reader into communication with a victim which is very far away. A pick pocket system can be used by the attacker to use the contactless card data of the victim without the knowledge of the victim. NFC stands for Near Field Communication in which three types or modes of operation are possible. They are card-emulation mode, peer-to-peer mode and read/write. In the mode of card emulation, the Near Field Communication device will emulate as a contactless smart card. While in the peer-to-peer mode, the NFC device will communicate with the payment system reader directly. The last is the read/write mode in which the NFC devices communicate with the Near Field Communication (NFC) tag (Kfir & Wool, 2005). NFC relay attack can be achieved by a peer-to-peer communication channel, a verifier which is malicious (fake terminal) communicating with the contactless payment card which is legitimate and a malicious prover (fake card) which communicates with the legitimate Point of Sale (POS) terminal.

The legitimate card makes the communication which is relayed to the legitimate terminal without the knowledge of the cardholder to a malicious prover and a malicious verifier. There are certain limitations to this attack which are that the device which is enabled with Near field communication acting like a malicious verifier must be in the
read/write mode (Kfir & Wool, 2005) and also the card should be in host-card emulation mode (HCE) which is supported natively from Android KitKat onwards (Kfir & Wool, 2005).

For performing this attack successfully, two off-the-shelf mobile devices which were running Android and have the Near Field Communication enabled executing an Android application were built for the purpose of testing (about 2000 JAVA lines of Code Counter [LOC] and which were able to work as a dishonest prover/verifier, depending on the choice of the user). They have one constraint that the device which is the dishonest prover should execute Android KitKat version at least (Kfir & Wool, 2005). Ingenico IWL280 is the device used as the Point of Sale device. Several devices like Nexus 4, Nexus 5 were used as dishonest provers and devices like Samsung Galaxy Nexus, Sony Xperia S were used as the dishonest verifiers for testing the experiment (Kfir & Wool, 2005).

NFC-enabled passive relay attacks can be avoided by using Faraday-cage approach. Another countermeasure is by controlling the activation of the card which gets activated only after the entry of Personal Identification Number (PIN) by the owner of the card.

Another major attacking technique on EMV cards is called Shim in the middle attacks. These attacks involve the insertion of a flexible and very thin circuit board between the card chip and the reader into the card slot. If a signal is transmitted by the circuit to the receiver nearby, it is very hard to detect in the PED. A shim can also be attached to the card by the attacker and then be inserted into the PED. Attacker can
remove the inserted card and the shim stays in place inside the machine. The card
details and the PIN’s (Personal Identification Numbers) are recorded by a nearby
receiver. If the PIN was sent in the plain text then the PIN (personal identification
number) of the cardholder can be intercepted (Bond, 2006). With the use of the
intercepted information which is related to the account or the Personal Identification
Numbers (PINs) magnetic stripes can be counterfeited which can then be used later for
the purposes of unauthorized transactions at the terminals which accept the cards with
the magnetic stripe. This attack does not need the participation of the employee.
Hence the merchants who are corrupt prefer to do this as they can deny about
the knowledge of the existence of the shim in their PED with ease.

Obeying the PCI DSS goals can help the merchants in preventing this attack.
Owner of a card can prevent this attack if he/her have the knowledge of detecting the
presence of a shimmer inside the terminal. Even the merchants can help by training
their employees about the possible attacks and use the terminal which has tamper-
resistance to prevent this attack. Even during the daily inspection routine, POS clerks
can also identify any alternations to the Point of Sale (POS).

Eavesdropping means secretly obtaining information without getting identified. In
the process of an EMV transaction at the Point of Sale terminal (POS) the Personal
Identification Number (PIN) or the details of the account can be eavesdropped for
forging the magnetic stripe to be used in fraudulent activities. There are many kinds of
Eavesdrop attacks. Some of them are Camera and Double-swipe methods, Counterfeit
terminal and signal Eavesdropping attack.
Camera and double swipe method involved a fraudulent merchant and a camera which faces the Personal Identification Number (PIN) pad. The fraudulent merchant swipes the card of the customer through his/her own device for intercepting information which is needed to counterfeit the magnetic stripe. The merchant who is fraudulent keeps two terminals in which one of them is a genuine terminal and the other one is a fraudulent terminal which requires the bypassing of a tamper resistant device. The process of tampering with the Point of Sale (POS) device is complicated and requires a lot of considerable manual effort (Bond, 2006).

In the approach of Counterfeit terminal, data is captured to forge the magnetic stripe. This counterfeited terminal requires the owner of the card to enter the PIN which uses the sensors or the software key loggers to intercept the entered PIN (Bond, 2006).

Signal eavesdropping attack is another kind of attack on EMV cards which is used to create the fake magnetic stripe card for which the information is gathered from tapping the data line in the PED. The data is captured which is unencrypted from the tapped data line in the PED. The demonstration of this attack was shown on two widely used PED devices in the UK which are the Dione Xtreme and Ingenico i3300 (Drimer, Murdoch, & Anderson, 2008). The Ingenico PED device i3300 device was very easily defeated with a fairly simple tapping attack as it had very weak design and many flaws. This PED of ingenico had a simple and very accessible rear compartment which was accessible for any user and moreover it was not tamper proof (Drimer et al., 2008). The circuit board is accessible through this compartment through which many signals are routed in the bottom layer. The designers of the Ingenico I3300 chose to give 1 mm
diameter holes and the other holes through the PCB which stands for the printed circuit board (Drimer et al., 2008).

These holes are important for positioning the surface mount sockets which are optional. A PED having one of these holes can be used easily for tapping the data line with the use of a metal hook. In between the chip of the card and the microprocessor, the tap can be placed. In this given case, the attack was easily achieved with the use of a bent paper clip which was placed through the hole (Drimer et al., 2008). Coming to the other PED device which is the Dione Extreme PED does not have a concealed compartment which helps to hide the wiretap which is an advantage but still it has a possibility and is vulnerable. Though, a needle of length 4 cm can be easily inserted through the hole on the rear side of the PED device into the flat ribbon connector socket. The hole on the rear side of the device is about 0.8 mm which can be used for making this arrangement (Drimer et al., 2008). The connection to the Field Programmable Gate Array (FPGA) board using a thin wire can do the translation of the data and then send it to an external device like a laptop which will show an answer to reset (ATR) which is the initial exchange that is intercepted using the tap (Drimer et al., 2008). In the Ingenico i3300 PED device, the attacker can easily record all the details of the transaction by inserting a FPGA (Field Programmable gate array) board which is very small and can be placed inside the PED device successfully without the knowledge of anyone. On the other hand, in the case of the Dione Extreme PED device, the small FPGA board which is the same size cannot be hidden inside the compartment as that of the Ingenico i3300 PED device. Hence the attacker must hide it under the counter and
usually cannot be easily detected unless the owner of the card knows about what he/she is looking for (Drimer et al., 2008).

The prevention of these kinds of Eaves dropping attacks is possible if the PED device merchants will comply to the PCI DSS goals which is “Protect Card holder Data and Implement Strong Access Control Measures” (Xilinx, Inc., 2009). There are even few cases of the eavesdropping attacks in which the merchants are themselves culprit and perform these kinds of eavesdropping attacks. Hence to avoid these attacks, the owner of the card must be educated and tips must be given on how these eavesdropping attacks can take place and the ways in which the modifications to the payment terminals can be detected and thus protect themselves and others from falling into the traps laid by the attackers.

The EMV chip cards currently are very weak towards an attack which is called the fall back to the magnetic stripe in the case of the Chip and PIN not being used. This is very beneficial for the attacker. This helps the person performing the attack to easily grab the sensitive information and skim the credit card data and also record the PIN (Personal Identification Number) (Bond et al., 2014). With this information attacker has skimmed, he/she can create a new card along with the account data as well as the noticed PIN (personal identification number) to perform unauthorized transactions. Not only in the United States of America (USA), even the other countries which have adapted to EMV accepting the Chip cards along with the magnetic stripe have faced a problem with this approach. Hence, the attacker can then use this card which has stolen data from one country, in another country still using the traditional magnetic stripe
method for payments at their Point of Sale systems (POS). Since this attack involves
the use of fallback to magnetic stripe in another country or virtually anywhere, this
attack is the international version of the fraud and is also called as the cross-border
fraud.

The countermeasures for the fallback to the magnetic stripe-based credit card
attacks can be effective with the use of PIN’s (Personal Identification Numbers) which
are encrypted along with the use of ‘iCVV’ which stands for card verification value for
the integrated circuit cards. The traditional cards which store the CVV (card verification
value) is replaced by the new iCVV (card verification value for integrated circuit cards) in
the chip cards. When the cards perform the EMV transactions using the iCVV code, the
CVV value can be extracted from the magnetic stripe when the card is swiped into a
separate card reader (Drimer et al., 2008).

Active Relay attacks are a kind of attacks which weaken the EMV Chip and PIN
card transactions. This attack involves an attacker who installs a fake card reader and
makes the card holder initiate the transaction process of EMV without the knowledge of
the victim who thinks the terminal is safe and transaction is secure. The card holder
thinks that the transaction he is making is for a small amount at the malicious reader
whereas the fraudulent reader actually relays the response of the card to a legitimate
reader which is remote and is used to pay for items which are more expensive
(Mehrnezhad, Hao, & Shahandasthi, 2015). The information which is relayed through
the wireless communication allows the Point of Sale (POS) purchase. The card holder
who is the victim does not know about the expensive transaction that was made.
He / She thinks that they have made a purchase for the small amount but eventually they would be billed for the transaction which is much larger. As the malicious reader which was used for the transaction is not legitimate and not connected to any bank, the victim will never be charged for the small amount purchase transaction he made and only the transaction made with large amount is recorded (Drimer & Murdoch, 2013). Both contact and contactless EMV transaction can be hacked using this attack which depends on the compatibility of the card and the Point of Sale system (POS).

This kind of attack requires both the fake terminal and also the fake card. The board which is used in the fake terminal is an FPGA (Field Programmable Gate array) board (Drimer & Murdoch, 2013).

These kinds of attacks can be prevented by using either a user interface or also a distance-bounding protocol can be used to tackle the Active Relay attacks. In the use of an UI (User Interface), the card owner inserts the card into the interface terminal. If the amount that is shown on the User Interface is satisfactory to the owner of the card, then the card owner can proceed and perform the transaction otherwise they can abort it. By using the interface, the transactions can be protected from the forging of magnetic-stripe card data. To implement the distance bounding protocol, both the card and the terminal should support this protocol (Drimer et al., 2008).

All these kinds of attacks can be summarized with the Attack Tree methodology which can be used to show the various ways in which the system can be weakened and aid in designing the countermeasures to these attacks (Schneier, 1999). Different attacks towards a system are visualized as the goal and the various ways in which it
can be attacked is displayed using the leaf nodes. All the leaf nodes transform into a sub goal and the children of these leaf nodes lay the path to reach the sub goal (Schneier, 1999). The refinement of the attack tree structure is achieved using the logical connections which are OR or AND. The OR logical connections play the role as the alternative methods whereas the AND logical connections requires all sister node conditions have to be met for reaching the sub goal. In the attack tree figure, the OR logical connectors are simple line connectors while the AND logical connection is shown using "\( \land \)".

Below is the table which lists the EMV attacks. The arrow vector is used for representing the down hierarchy of the nodes of attack tree. This basically means the sequence which the attacker must follow for achieving an attack. The logical connection AND derived from the attack tree configuration is shown in the table as the ampersand (‘&’). For the case of the logical OR connection, the representation is done using (‘¬’) notation. The attack tree figure is followed after the table.
### Table 2


<table>
<thead>
<tr>
<th>ATTACKS</th>
<th>Attack Tree Nodes</th>
<th>Attack Mitigation Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Man-in-the-middle</td>
<td>1 -&gt; 1.1 -&gt; 1.1.1 -&gt; 1.1.1.1</td>
<td>Cardholder gets real time notification of the transactions made. Merchants inserting cards into the terminal by themselves. Card issuing bank signing the CVM list.</td>
</tr>
<tr>
<td>Attack</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pre-play Attack</td>
<td>2 -&gt; 2.1 -&gt; 2.1.2 -&gt; 2.1.2.1 &amp; 2.1.2.2</td>
<td>Cryptographically secure random number generator. Faraday-cage approach. Signed CVM list.</td>
</tr>
<tr>
<td>NFC-Relay Attack</td>
<td>1 -&gt; 1.3</td>
<td>Faraday-cage approach and controlling the card activation</td>
</tr>
<tr>
<td>Attack</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 2 (continued)

<table>
<thead>
<tr>
<th>Method</th>
<th>Steps</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Camera and Double-swipe method</td>
<td>2 -&gt; 2.1 -&gt; 2.1.1 -&gt; 2.1.1.2 -&gt; 2.1.1.2.1 &amp; 2.1.1.2.2</td>
<td>The cardholder having adequate knowledge about how to detect the modification in the terminal and to determine suspicious activities.</td>
</tr>
<tr>
<td>Counterfeit Terminal</td>
<td>1 -&gt; 1.2 -&gt; 1.2.1 &amp; 1.2.2 -&gt; 1.2.2.1 – 1.2.2.2 – 1.2.2.3</td>
<td>Encrypted PIN and use of ‘iCVV’ (i.e. ensure the transaction is chip based)</td>
</tr>
<tr>
<td>Signal Eavesdropping Attack</td>
<td>2 -&gt; 2.1 -&gt; 2.1.1 -&gt; 2.1.1.1 -&gt; 2.1.1.1.1 &amp; 2.1.1.2</td>
<td>PCI DSS requirement: Encrypt transmission of cardholder data across open, public network and restrict physical access to cardholder data. The cardholder able to detect the modification in the terminal.</td>
</tr>
<tr>
<td>Active Relay Attack</td>
<td>3 -&gt; 3.1 &amp; 3.2</td>
<td>Distance-bounding protocol of card and terminal and/or user-interface method.</td>
</tr>
</tbody>
</table>
Figure 3: Attack tree modelling at POS (Reprinted from Schneier, 1999).
Even the customers are in a state of confusion as they do not have an idea of whether they have to swipe their credit card or insert it. Following that they have to do a signature or enter a PIN all leading to a confused state where the customers have to deal with long lines and even the staff are taking time to get acquainted with the transaction process (Hamblen, 2016). They are also facing troubles for using options like apple pay, android pay or Samsung pay where one has some tedious steps to perform in the phone. The Samsung Pay uses the virtual magnetic stripe for some situations to make payment but it fails sometimes and will tell you to use the chip on the card. There are even similar issues with the Apple Pay and Android Pay.

**Literature Related to the Methodology**

The EMV cards emerged with the promise to solve the issues that were prevalent with the use of magnetic stripe cards. Unfortunately, after the launch of the EMV cards in Europe in 2003 there was a rise of different kinds of frauds other than those which were found with the stripe cards. There was a significant increase in the card-not-present frauds. Criminals adapted two ways where first they moved to card-not-present frauds. The graph in Figure 3 clearly shows the significant rise of card-not-present attacks through the Internet, mail-order, phone-based payments which were beyond the scope of the EMV cards. The second was that they started making magnetic-strip clones. The skimming attacks were always being done by hackers where they install some devices on the throats of ATMs which could capture card data and also record PINs. Now the PINs were demanded almost everywhere not just at the ATMs which lead to the increase of these skimming techniques widely. The deployment of EMV
along with the magnetic strip means the fallback and the backward compatibility features of the EMV could be exploited. Though the UK phased out the usage of magnetic strip cards in ATMs for locally-issued cards, it was possible for hackers to create a magnetic stripe clone of the UK cards and use them in the USA. This was the reason for counterfeit fraud going up even after the UK EMV roll-out in 2005. The customers used to enter PINs only at ATMs, but now they are entering them even in the POS terminals which are even much easier for tampering (Bond et al., 2014).

**Figure 4**: Fraud levels on the payment cards (Reprinted from Financial Fraud Action UK, 2014).

Relay attacks and Skimming attacks significantly increased. This led to identify and summarize the attacks that took place after the use of the EMV cards. EMV cards claimed to be foolproof from cloning and interception, but after a conscientious study by the hackers they could do fraud with the EMV cards (Ahmad, Zeki, & Olowolayemo, 2016).
EMV was a powerful move to increase the security of the payment cards which could overcome the frauds which were occurring due to the use of magnetic stripe cards. But even with the implementation of EMV cards there was an attack which exposed that there was a protocol failure and the main essence of the system "verified by PIN" was not working. Hence, they considered the chip and PIN system to be broken. It was found that EMV was weak against replay attacks and card-not-present frauds. They also found that the PIN accepting POS terminals had inadequate tamper resistance (Murdoch et al., 2010).

The frauds were one face of the coin concerning the failure of EMV chip cards. But there is also another face of the coin which was an important factor that laid path towards the failure of EMV implementation which was lack of awareness in consumers. Based on a report released by HarborTouch, which is a leading national Point of Sale (POS) system and also a merchant services provider which conducted a large-scale national survey focusing on consumer awareness and usage trends of EMV or can be called as the chip-enabled credit cards. The survey which involved the responses from 18,000 U.S adults conducted in late August 2015 had identified that 56% of consumers were not even aware of what an EMV or a 'chip' credit card is. Digging deeper into the report, respondents having lower income were more likely to lack knowledge of the chip cards when compared to the respondents making higher income brackets. Respondents making an income of $25,000 - $49,999 were not aware of the EMV cards. Only 26% of the respondents earning higher income (earning more than $150,000) lacked knowledge about the chip credit cards. This highlighted the need of educating the
consumers about the chip cards and also the transition which would arrive shortly from old-fashioned 'swipe' credit cards to the EMV or 'chip' credit cards. On 1st of October 2015, payment networks including the VISA and MasterCard will shift the liability for credit card fraud onto the merchants of United States of America who will not be adopting the EMV chip cards as their principal method of credit card payment. The report also shredded focus on the various usage trends of the EMV chip credit cards among the U.S.A consumers. More than half of the respondents (53.6%) told they did not receive any replacement EMV cards or the 'chip' cards from all of the providers of credit cards highlighting the late arrival of the new EMV cards. More than the urban residents, the rural dwellers were leading in the usage of EMV credit cards. 64% of the urban respondents have reported that they were using EMV credit cards when paying for the goods while 76% of the Rural respondents have reported usage of EMV cards. Another interesting finding was that the younger age group which were the respondents in the age bracket of 18 - 24 years, also called as Gen Z, were very less likely to use the EMV chip cards (only 20.5%), while they reported the highest usage of mobile payments which is 42.1%. Only half the percentage of respondents believe that the upcoming implementation of the EMV 'chip' cards will make them more secure. Although the payment networks trust and believe the security benefits of EMV, only 50.8% of consumers felt that this implementation of technology would make them more secure. Only 41.4% of women believed in the security of EMV cards, while 58.8% men felt it secure thus concluding that more percentage of men than woman felt secure about the EMV credit cards (Report: More, 2015).
Another survey conducted by BRP which was the 19th Annual POS/Customer Engagement Benchmarking survey was held in November and December of 2017 (Survey, 2018). More than 500 top North American retailers were contacted to understand the gaining of retailers’ initiatives planned, their priorities and the future trend. The findings of the survey gave an insight of the client experience and the overall retail experience. It also summarized the current and future trends in the industry. Of the total survey respondents, the primary retail respondents of the survey were specialty hard goods which occupied 28%, and the next major respondents fell into the category of hard goods holding 26%. The remaining respondents fall into various other categories like grocery, beverage, food and general merchandise. The specialty hard goods and the soft goods are two major classifications in the retail industry. Soft goods can be termed as the goods which mean they are literally soft like bedding etc. while the hard goods are referred to like the ones which are less personalized like the home appliances etc. They are mostly referred to as consumer durables (Maverick, 2018).

Below is the figure comprising of the wide varieties of respondents took part in the survey.
According to the survey, EMV implementation has not been fully adopted. It states that, though the introduction of EMV through Liability shift has exceeded more than two years, many retailers have not implemented the EMV (Europay, MasterCard and Visa) yet. The retailers are still working on providing the transactions which are enabled through EMV. The further acceptance of this new standard of EMV is visible as the growth of EMV transactions have risen to 59% in the year 2017 when compared to that of the 52% in the last year survey of 2016. While the numbers are increasing but there are still many more retailers that have to shift and implement the EMV payment standards for EMV to go live up to full extent (Survey, 2018).

In the survey, retailers and customers in the stores have realized that the average time which is taken to complete a transaction which is enabled through EMV is much longer when compared to that of the transactions made through the traditional
magnetic stripe method. In the majority of stores, long processing times can cost more for the retail stores as they have to increase in the number of lanes for check out and also need more staff than usual so that the wait times of the customers are manageable (Survey, 2018).

With the implementation of EMV, they found that there is a significant reduction in the ‘in-store’ fraud but the online fraud which also includes the mobile applications have grown dramatically. Hence it becomes more important for retailers to secure customer data and successfully monitor online and in-store transactions. Below is a figure explaining the payment security technology plans among the retailers.

**Figure 6**: Payment security technology plans (Reprinted from Survey, 2018).
The survey has highlighted that Mobile payments give more opportunity for retailers as well as customers because it provides the customers the ability to make purchases without their wallet. Although it can happen only if they carry their mobile devices also termed smartphones which offer more security than that of the traditional credit cards or the cards with a chip, 'EMV cards' as they add an additional layer of security. Apple Pay and PayPal continued as the widely accepted payment types according to the survey. But fewer retailers are adopting the wait and see method compared to the last year as the support for the payment software ecosystem and the acceptance of mobile payments in public is rising. The wait and see approach is basically that the retailers have not taken any decision towards adopting mobile payments but tend to analyze the market in the field of mobile payments.

Below is the figure showing the adoption of retailers towards mobile payments and future plans for the adoption of alternative payment types (Survey, 2018).
Summary

This chapter covered the background related to the EMV system. The advantages of using the EMV cards over the traditional magnetic stripe cards. The reasons for the failure of EMV and about the possible frauds possible with the EMV cards had been highlighted. The literature related to the EMV cards and their background was discussed. Finally, the literature related to the methodology of the EMV systems had been focused. At this stage, the paper describes the background of the problem and discusses the literature works that were done regarding the issue. The next chapter focuses on the methodology of the study that will be implemented to gain
data for analysis and derive the problems of the existing system thus provide alternatives to it.
Chapter III: Methodology

Introduction

The design for research implies the plan in which the research should take place. This chapter focuses on choosing the design of the study and the reason for choosing a specific design over the others. It also discusses the techniques used for the collection of the data and the tools used for collecting the data along with its details. Finally, this chapter covers the work in progress and a timeline of the events which could determine the estimated time for the completion of the study.

Design of the Study

The research design is about planning an overall strategy which combines the different parts of the study logically to address the research problem effectively. In this paper, a mixed approach is very effective to address the issue related to the security of the EMV cards and to identify the future payment methods which are reliable and safe. The qualitative approach for this study is required to acquire the opinions, motivations and the reasons underlying it. This type of research helps us to get a more detailed understanding of the problem and gives us aid in identifying trends and plunge deeper into the problem. The quantitative approach for this research is essential to find the patterns and generate data which can be converted into useful statistics for obtaining a generalized result from a bigger sample population. This method uses different methods like online surveys, mobile surveys, etc. for collecting the data which can be used to identify the trend and obtain a clear picture of where research must be focused.

Choosing the mixed approach over only qualitative or quantitative approach ideally
covers the sap of the two research approaches and is essential for identifying the success and reliability of EMV Chip and PIN cards implementation.

**Data Collection**

The collection of data is done in different methods. The data collection methods which will be used for this research include a survey and information from the internet. There are many articles related to the chip card security and information related to various payment methods used along with their reliability are available on the internet. There are several articles about the future payment methods and current threats being faced by the payment systems. There are even conferences which are held yearly to discuss the security regarding the security systems, discuss and provide solutions to the threats and identify new threats to the system. IEEE is a standard which conducts conferences around the world and gives a platform to present the latest technologies in papers which can be used for publication in journals.

**Tools and Techniques**

The tool used to collect the information for the survey is called Google forms. It is a software provided by Google which aids in conducting surveys online. It is a cloud-based software which is free to use through a browser and also has a mobile application supporting Android and iOS. It offers survey solutions with real-time collaboration and powerful tools which help in customizing the questions for the survey. It also has analytics capabilities and provides with beautiful and vibrant pie charts and bar graphs using which data can be analyzed graphically and formulate solutions through data collected from the survey.
Summary

In this chapter, the methodology of the paper is discussed. It highlights the design of the study in which the mixed approach is used to find a solution for the EMV cards. The reason for choosing mixed study methodology over other methodologies is discussed. The mixed approach involves both qualitative approach as well as the quantitative approach. Also, the different ways in which the data is collected using a vast variety of sources is highlighted. These include but not limited to survey, existing research, IEEE papers and many more. Lastly, it highlights the tools which will be required to conduct the survey and the aid required for the analysis of data is mentioned. This chapter on a high level discusses about the design of the data collection and tools which will be necessary for acquiring the data and analyze the resource collected. The next chapter will include all the data which is collected on the survey and various kinds of analysis that will be done to identify the patterns and give a precise understanding on the ways in which the data can be used to answer the study questions of this paper.
Chapter IV: Data Presentation and Analysis

Introduction

Data is a powerful term. Any meaningful information is called data, and its collection is called data collection. Any organization or process needs to analyze and process the data for understanding the quality of information and take insights for the future success of the organization and improve the efficiency of the process. The EMV chip and PIN cards implementation has started, and many flaws have been identified, while it was considered to be foolproof and secure. In this paper, various flaws and defects of the implemented EMV technology has been identified. Hence to cover the gap in the practical sense, data is collected from the various participants involved in the EMV usage and the data is analyzed to get a bigger picture to understand the implementation of the advanced EMV system and its success.

In this chapter, the data that is collected through the process of the survey is presented. Then the data gathered is analyzed, and meaningful insights of the data are uncovered. This analysis of data helps in understanding the success of the EMV on an overall sample of data collected and useful information is collected. Finally, this chapter concludes about the summary and facts of the collected data.

Data Presentation

To understand the implementation of the EMV chip cards and measure its success, an online survey has been conducted using the Google forms cloud application which helps in conducting surveys. While planning for the survey, some decisions had been taken to carefully craft the questionnaire so that the information
needed to answer about EMV is sufficient to analyze the EMV implementations and also answer the study questions of this paper. Population limit of the survey was set to 100, a decent figure to analyze the data and derive a general understanding of the EMV implementation. The questionnaire had to be answered by the participants of the survey in the form of multiple choice questions rather than written answers so that the participants need not spend much time and quickly complete the survey. Often long surveys which collect data in the form of written texts are of less interest to the participants and also tricky for data analysis. Hence, the questionnaire was designed in multiple choice questions that are quick to answer, and the data can be used for analytics and analysis is quick and effective. The questionnaire comprises of 15 multiple choice questions each having reasonable options to choose from, for the participants. All the questions must be answered in order to submit the response. Through this takes away the freedom from the participant to skip but all the questions are given reasonable options to avoid answering to a point. Hence, by placing this rule, all the 100 responses collected will be equal and occupy a fair share while making the analysis. It has two sections in which the first comprises of the demographic information about the participants and also the high-level questions about EMV card. In the second section of the survey, the questions are based on the Modes of payments and their preferences are collected. Please refer to the Appendix, Survey Questionnaire to find the questions used for the survey.

The survey took about a month to gain 100 responses while the survey has been posted on many online blogs and used social media to distribute the link. Since it was a
free survey without any rewards, the time taken was longer for this sample when compared to many surveys which provide rewards for completing them.

The data collected through this survey was exported from the Google forms applications in the form of a CSV file. All the data in a CSV file is comma separated values tailoring responses in the form of a list for all users, ordered by the questions on the top. The CSV files can be opened in an editor like Microsoft Excel which provides a neat and concise view of the whole data. Below are the screenshots of the responses in the Microsoft Excel where each screenshot below has the responses of 50 participants.

![Survey responses of 1-50 participants](image)

**Figure 8:** Survey responses of 1-50 participants.
### Figure 9: Survey responses of 51 - 100 participants.

#### Data Analysis

On the vast amounts of data acquired using the survey, statistical analysis is performed on the data to identify the patterns which give more information about the EMV cards and its current situation in the market. For analyzing the data, a feature of Google Forms was used that use this data to create statistical charts and give deeper insight on the responses from the survey. Below are the statistical images of the survey data. Since all the data acquired have responses from each participant, the data is more efficient though the population limit for the survey is set to 100.
In this survey, out of all the participants of the survey the male constitutes 52% male, 39% female, 8% preferred not to say. (This option was added since all questions are mandatory and had to give neutral choice for people who prefer their privacy.)

**Figure 10**: Survey report Q1.

**Figure 11**: Survey report Q2.
The age group was important as the usage of cards varies by age and people are more financially stable in the later ages when compared to the growing age. Forty-three percent of the participants of the survey were aged between 25-45 years which is a good sign where most of them use the cards and have relatively more knowledge when compared to the other age groups. The next leading age group is 15-24 years which occupy 40%, is relatively close to the 25-45 years age group whose responses are valuable as they are of prime age and will be using the technology more in the coming years. The age group of > 46 years are usually well settled and can give an idea of how educated people are about the new technologies implemented like the EMV Chip and PIN cards. Under 15 years age group constitutes about 2% who also use the chip cards as the minimum age in the USA to have a debit card is 14 years, but they have their limitations.

![Pie chart showing degree distribution](image)

**Figure 12:** Survey report Q3.
In general, the higher the education level more is the knowledge gained in society and have more acquaintance and concern regarding security and privacy when related to financial matters. This survey population comprises of 48% participants having a master's degree, 25% of them completed their bachelor's degree, 7% completed their doctorate while 5% have an associate degree and 12% of them have high school degree measuring to 97% of them being educated brings more quality to this survey. Financial management is an integral part of life and being secure and aware of the latest technologies implemented in securing them is vital. The survey calculations will measure almost near to the average of the surveys which involve a larger population sample while conducting surveys.

![Pie chart showing employment statuses](image)

**Figure 13:** Survey report Q4.

Employment status gives more detail about the working nature of the participants of the population. While only 3% of the entire sample preferred to hide their employment
status, all the other sectors of this chart representing various employments give an idea about the usage of the EMV cards in the diverse lifestyles of the population of the survey. Majority of the participants in the survey are workers who are employed for wages while the other significant pies of the chart are occupied by self-employed workers and students holding 22% and 19% respectively. Even though the other portions are occupying less in the charts, EMV cards are used by most of them and having the insight from them is valuable to calculate the awareness and effectiveness of the implementation of the EMV chip cards.

**Figure 14:** Survey report Q5.

The above chart highlights the extent of knowledge people have about the EMV cards and what exactly it is for. Many people do not know what the cards are, even though they are using them which highlights the lack of awareness of the EMV chip cards. It is a good sign that 52% of the participants which is higher than half of the size
of the sample answered as Yes which states that many people have heard about the EMV chip cards. Even though 36% of the participants have responded that they do not know about EMV cards, which being less when compared to the population who have knowledge of the EMV cards. 36% is not a small chunk that can be omitted and also, 12% are not sure whether they know or not which can also in a sense be counted into the group of participants who do not have knowledge of the EMV cards summing to 48%. This chart showing high numbers highlighted that people are not having much knowledge of the Chip and PIN EMV cards.

![Pie chart](chart.png)

**Figure 15**: Survey report Q6.

This chart highlights the successful implementation of EMV. The liability shift took place on October 1, 2015 and still even till the date of the survey which is in March 2018 about 41% of the respondents say that they have not received EMV chip cards from all the financial institutions which is way past the liability shift due date thus showing that
financial institutions are taking very long time to issue the Chip cards. The financial institutions have to take action by contacting the customers on providing the new type of EMV chip cards which is more secure but the time taken by the financial institutions to issue the EMV cards is very long when compared to the scheduled liability shift.

Figure 16: Survey report Q7.

As time passes, retailers and stores have offered various methods of payments to their customers. Seeing the chart above it clearly states that most of them are aware about the traditional swiping cards constituting to 93% which most of them use on a regular basis for paying expenses. The EMV cards though have been implemented long before Mobile payment services and NFC payment services, still only 66% of them heard about this payment mode when compared to that of the Mobile payment using services like PayPal and NFC payment services which include Apple Pay, Android Pay etc. which stand at 85% and 70% respectively. Cryptocurrency is a relatively new
method of payment and is not widely used. Still, about 43% of the participants know about this form of payment. Though it had been a hard time for the rise of cryptocurrencies but are on the verge to come to an end soon. Another interesting observation is that Mobile payments using private services and NFC payments are increasing in popularity, and people are adapting to them because of the ease of using those technologies. Also, they are fast and secure when compared to that of the EMV chip card technology which take longer time to perform payment and also vulnerable towards the attacks. Since, Mobile payments and NFC are rising next to the traditional swiping cards, if the focus shifts towards the improvement of security towards Mobile Payments and NFC services, people are more willing to adopt towards these modern methods of payment.

In the bar graph, it is observed that 66% of the participants have responded that they heard of EMV cards while the survey report of Q5 states that only 52% of them heard about it. This question was setup for cross verification to observe the reliability of the survey. This implies a small deviation about the responses of the survey and gives insight about the confidence in the data used for building the survey report and conclusions around it. The quality of the survey data cannot be counted as 100% accurate but has some deviation so that the reader can have an insight on the confidence of data and are aware about it.
With implementation of the liability shift, it is up to the retailers to implement the Chip card technology for payments at their stores. Otherwise, the liability in case of any fraud is the responsibility of the store and not the financial institution. Not shifting to EMV pose a risk to the customer data at the Point of Sale terminals in the retail stores who make payments at stores which do not use the chip for payments. Even the retailers who opted for chip POS readers do not have the POS devices. Though many have it, many financial institutions have to approach the retail store to verify and start the usage of the specialized EMV enabled POS devices which are taking very long to complete. This chart highlights the successful implementation and the active usage of the working EMV enabled POS terminals. According to the Pie chart which explains about the working payment options customers find at most of the retail shops show that

**Figure 17**: Survey report Q8.

What kind of payment options do you find at most of the retailers you visit and are working?

- 58% EMV chip cards
- 24% Traditional POS machines accepting card swipes
- 11% NFC payments (Eg. Android Pay, Samsung Pay, Apple Pay etc.)
- 7% Only Cash

100 responses
58% of the store's customers visit still rely on the traditional swiping cards for the payment at the store. Only 24% of the stores which customers visit say that the EMV cards are working which is very less. Due to this implementation of different payment forms at stores, customers are left at the point of confusion and are not sure of which payment method to use unless they reach the billing area of the retailer and guided by the representative of the store for payment. This clearly states that EMV has not been fully enforced at most of the stores which can be estimated by the figures obtained on the pie chart above. The other forms of payment include NFC payment which customers are sure at their retailers to have this payment method working. There are even some small shops and retailers who do not accept credit/debit cards and rely on cash for performing a financial transaction between the store and the customer. Due to the vast usage of the traditional swipe technology for payments, they impose a risk for customer data while the secure EMV implementation did not take place efficiently. Various kinds of attacks on EMV cards could be performed with little modification to the secure EMV cards and using them at the retail market stores which did not shift yet or are in the process of shifting to the EMV, still using the traditional swipe method impose risk to the card users who upgraded to the EMV chip cards.
Above data highlights the use of EMV cards and the level of comfort users of the EMV cards have with EMV technology. It shows the confidence of the people using EMV cards and their desire to stick to the new form of payment. Of the entire sample, only 31% of the participants believe in the use of EMV cards and are confident of it working in any retail store they visit. While a larger chunk (36%) of candidates still doubt the working of EMV cards at any retail store they visit and still prefer to use the traditional swipe cards due to lack of perfect implementation of the EMV chip card technology. The percentage of users using the EMV should rise to increase the trust in the EMV chip and PIN cards to say that it is implemented successfully. One more interesting fact observed in this chart is that mobile payments though being less when compared to the EMV and traditional payment methods, 22% is a considerable number. With the right awareness and improved security of mobile payments, the customers...
tend to move over to the new technologies, once the customer’s confidence is boosted on the safety and ease of usage of the payment method.

Figure 19: Survey report Q10.

The Chip and PIN cards take longer time to process when compared to that of traditional swiping card technology for payments at the stores. Significant amounts of time had increased at the billing counters to process the financial transactions. However, the end user who is using the EMV chip cards should have comfort as they are the ones for whom it was built for and also keeping security in mind. This pie chart shows that 44% of the total sample population is comfortable with the time taken while 32% are not comfortable with the long delay at the stores. Even though the majority of the participants being comfortable with the processing time are accepting it shows it as a good sign, but the rest 32% and also who are in the state of confusion should be kept in mind and efforts have to be taken so that this processing time decreases in the
coming future. At the whole people might not be comfortable waiting longer at stores to get their turn for payment. Hence stores must also increase the workforce and also increase the required number of terminals so that customers can get work done quickly and keep going.

![Pie chart](image)

**Figure 20:** Survey report Q11.

Although the use of EMV cards is significant, the market has always kept moving towards implementing new technologies for secure payments and keep the life of consumers easy and quick. The use of mobile payment services like Android Pay, Apple Pay, and many more services have increased rapidly with the advancement in technology and mobile devices. Even there are other devices like smartwatches which enable to perform transactions using these services through NFC payment capabilities built in them. Of all the participants of the survey, 62% of them have used these payment services at least once which is a massive chunk of the sample when compared
to the users who have not used and are not sure about this form of payment technology which comprises to 38% combined. This stands as good news as people have started using mobile payments for their day to day activities and is the next more secure option to the EMV chip and PIN cards. The NFC payment method is more secure and performs significantly fast when compared to that of the EMV chip and PIN cards. This chart specifies the popularity and the extent of adaptation that took place in the field of NFC payments and helps us gain a better understanding of the alternatives for the EMV chip cards to provide more reliable and fast service to the consumers.

**Figure 21**: Survey report Q12.

The EMV chip and PIN card implementation was to provide day to day payment transactions more secure and protect the user from any fraudulent activities. This pie chart represents the preference of a user (sample population) for the daily financial transactions they do using various payment options available at the stores. Of all the
popular payment methods found at most of the retail stores, only 22% of the participants of the sample responded to choose EMV cards for routine day to day payment activities which is relatively less to the most significant chunk in the pie occupying 36% opting towards the Magnetic stripe cards. Though the magnetic stripe cards are less secure, many prefer this payment as it is quick, available at almost any retail store or also could be due to lack of their knowledge on the EMV chip cards and its security. Hence steps need to be taken to increase the efficiency of EMV cards which are more secure than the traditional swipe cards. In this pie chart, mobile payments and NFC combined occupy 32% which is also more than EMV chip card users preferences stating a significant rise in these technologies and focus has to be shifted on improvising these payment methods which cover the defects of the EMV cards.

![How secure do you feel about using the Chip cards over traditional stripe cards?](image)

**Figure 22**: Survey report Q13.

EMV chip cards were built to keep consumers safe from fraud in their financial activities. It is always about the satisfaction of the end user to measure the success of
an implementation which is EMV in this case. This pie chart highlights about how secure the end users feel about the EMV chip cards. In the sample population, 31% of the participants feel the EMV implementation is very secure about EMV cards. While the most significant chunk in the pie is 42% of the participants feel somewhat secure as they lack about the knowledge of the security features implemented in the EMV cards. While 20% are not sure about the security or either they do not care about it. While 7% doubt about the security which is very less compared to all other categories in the participants. Right education has to be given about the EMV cards so that people are aware of what they are using and the number of participants feeling secure will rise, making EMV much stronger and reliable.

![Pie Chart](image)

**Figure 23**: Survey report Q14.

The EMV chip and PIN card implementation is all about making more secure transactions to the consumers in the day to day life. This chart highlights the frauds that have affected consumers. It is good that the most substantial chunk which is more than
half, 51% of the participants say that they were not involved with any fraud while using the EMV chip cards. 13% of the participants reported that they were involved multiple times in the fraud which is low. Ideally, having zero fraud is success, but no system is perfect, and consumers will have to be cautious from being involved in the scams. 18% of them have reported that they were involved at least once while the remaining 18% are not sure about it. Hence, people have to be educated about the security of EMV's and raise awareness to keep themselves secure from fraud.

![Pie Chart]

**Figure 24:** Survey report Q15.

This pie chart shows the trend public are following and get an idea to target security growth in accordance to the preferences of card holders. Out of the total participants, 45% of them choose to go for retail stores for the purpose of shopping in which mostly EMV POS devices and NFC payment options are available apart from cash. Hence focus should be in implementing more security and quick response around EMV chip cards and NFC payments. The next bigger chunk in the chart is 29% who
choose to do online shopping in retailer’s website. Hence security implementation in the websites have to focus on security to avoid Card-not-present attacks which utilize the information of the card and having weak encryption implementation of security data could be prone a risk to the card holders and high chance of getting involved in the fraud. 9% of them use third party websites for shopping and care has to be taken similar to retailer’s websites to avoid fraud. 17% of the participants are not sure while they can spread among any of the other 3 categories. Hence, it clearly states that EMV chip cards and NFC payments must be more secure and since websites do not use EMV, there is a higher risk of fraud and implementations have to be improved to provide security for online transactions. While still the larger population still go to the retail stores and hackers may tamper the POS devices, there is a higher chance of fraud and customers need to be more educated and be aware of the payment systems they are using and be vigilant about securing the card data from hackers.

**Summary**

In this chapter, the data presentation and statistical analysis of the data is covered. Initially, explanation was provided on the formulation of survey which included the decisions taken including the number of questions, type of questions for acquiring maximum and efficient responses is discussed followed by the reference for the survey questionnaire in the paper. Later, all the data that was collected from the survey was extracted in csv format and the data is displayed using the Microsoft Excel. Then this data is used to create visual charts so that statistical analysis can be done on the data. Later from each of these statistical charts useful information extracted is discussed and
important information is highlighted. Next chapter will discuss about the results and answer the study questions using the statistical data gathered in this chapter and conclusion will be drawn by the end of the next chapter. It will also cover about the future works of this paper and how the data from this paper can be used for further steps to be taken on improving EMV implementation and highlight about the alternatives to the EMV chip and PIN cards which are more secure and reliable to the consumers.
Chapter V: Results, Conclusion, and Recommendations

Introduction

EMV chip and PIN cards implementation was a huge step towards providing more security in day to day financial transactions of the consumers. In the USA, this implementation was a failure as the method of execution was weak. The liability shift is a failure step and due to which inconsistency of the platform took place and has made the situation worse. The research done in this paper is limited to EMV chip cards and give suggestions to better alternatives as well as to estimate the reliability of the EMV cards. This chapter will provide answers to the study questions based on the results and information gathered through the survey and will conclude the overall research done in this paper. It will also include about the future works and suggest on how to use the information gathered through this study.

Results

The study questions are useful in measuring the effectiveness of the EMV chip and PIN cards. The results will be explained based on answering the study questions by using the results of the survey and will give the conclusion based on the information identified in the results.

What are EMV cards, are people aware about them and do individuals possess the new EMV cards? The survey reports of Q5 and Q6 have clear representation to answer this question. Below are the survey reports of Q5 and Q6.
EMV cards are the new standard and an upgrade of the traditional swiping card mechanism for making financial transactions more secure and reduce fraud. EMV features a chip in the cards that store cryptogram which allows banks to determine if the transaction or card has been altered. The chip in the cards also has a counter which increments on each transaction to avoid duplication of counter values which indicate
possible fraudulent activities. In EMV, the customer authenticates a transaction by using their smart card which is inserted into a POS terminal and a pin is entered into the POS. Then the PIN is verified by the ICC (Integrated Circuit Cards) and is authenticated to the terminal using DS (digital signature) (Murdoch et al., 2010). Thus, making the cards more secure and can avoid fraudulent transactions.

The first pie chart from the survey report Q5 shows that 52% of the users of the survey population sample responded that they are aware of the EMV cards which is more than half of the total sample. 36% of the participants responded that they do not know what EMV cards are. 36% is not a small number that can be ignored and moreover the 12% who answered that they are not sure can also be considered that they are unaware, summing to 48%, which is a significant figure who are not aware of the new EMV payment method also keeping in mind that many of them still use it without the knowledge about it. Hence, it states that consumers have to be educated about the new payment technologies and its security. Also, awareness among people has to increase regarding the various kinds of frauds and ways to protect their financial data from being involved in the frauds.

What are the modes of payment used by individuals for their day to day transactions and their frequent mode of payment? The implementation of EMV is for the benefit of consumers. But it can only be successful if people prefer to use them in the day to day transactions like groceries, fuel, etc. With the survey reports of Q7, Q12 this study question can be answered effectively. Below are the two survey reports Q7 and Q12, respectively.
In the above survey report of Q7, it is clear that the most popular mode of payment is the traditional swiping of the cards for payment which is 93% as it has been in use since very long time and is the default payment method before the EMV chip and
PIN cards were introduced. EMV chip cards are reported by 66% of the participants and stands in the fourth place which highlights that people are either not familiar with the new technology or lack knowledge of EMV, even though many individuals are using it in their day to day payment activities. An interesting point here is about the mobile payments using the private services like PayPal is very popular and stands in the second place followed by the NFC payment services like Android Pay, Apple Pay, Samsung Pay, etc. standing in the third place moreover having higher acquaintance than that of the EMV cards. The NFC payments are a new technology for payments and people having huge familiarity can be considered as the alternatives to the EMV technology thereby giving tough competition to the EMV chip and PIN cards systems. Cryptocurrency has recently started to be used for the services and merchandise but will come to an end soon due to the decrease in the market value of the cryptocurrencies.

What type of authentication is preferred while performing card transactions by the individuals? EMV chip card is the new way to perform transactions at stores for the consumers to protect and secure themselves from getting involved in fraudulent situations. Failure of precise implementation of the EMV chip cards was because of the liability shift, there is a lot of confusion among the consumers at retail stores about which payment method to use unless guided by the representative at the counter. Though EMV is more secure, there is a vast usage of the POS terminals which only accept cards with the magnetic stripe, and also there are POS devices which have the new EMV feature to insert the chip cards but are still in the process of authenticating the
setup from financial institutions and rely on the magnetic stripe for payments. Based on survey reports of Q9 and Q10 this question can be answered clearly. Below are the two survey reports Q9 and Q10.

**Figure 29:** Survey report Q9.

**Figure 30:** Survey Report Q10
According to the survey report of Q9, only 31% of the users are sure about EMV chip cards and are confident to use them at any retail stores they encounter. While the highest number of participants chose to use the magnetic stripe payment method as it was the most widely used POS devices at most of the retailers and rely on it though it is less secure but quick in processing the transactions. In the survey report Q10, it shows that 44% of the respondents are comfortable with time taken by the POS devices to process transactions as they are more secure, while rest of the participants are not sure and are not pleased with the time taken during checkouts for processing transactions which are more than half of the total size of the participant sample which is a large number. In the survey report Q9, 22% of the participants opted for the mobile payments which is rising and if it continues to grow, it can be a reliable and quick payment method over the EMV chip cards.

**Do individuals prefer smart cards over magnetic stripe cards and how secure do they feel about using them?** Smart cards are another term for EMV chip and PIN cards. These new EMV cards are secure but take significantly longer time to process while the magnetic stripe cards are less secure but process transactions quickly. Moreover, due to the implementation of EMV chip cards through liability shift has caused many retailers still using the magnetic stripe and of all the retailers shifted to the EMV have the new POS terminals but still need time to process the authentication of their POS device from financial institutions. To answer this study question and analyze the consumer's preference between the EMV chip cards and the magnetic stripe cards the survey report Q12 can visually represent the answer and survey report
Q13 can visualize about how the consumers feel secure about the EMV chip and PIN cards. Below are the survey reports Q12 and Q13, respectively.

![Survey report Q12](image1.png)

**Figure 31**: Survey report Q12.

![Survey report Q13](image2.png)

**Figure 32**: Survey report Q13.

From the survey report of Q12, it represents that EMV cards are less preferred when compared to the traditional swipe cards. The survey report highlights about the
user’s preference for mode of payment in the day to day transaction, and it states that 36% of the users prefer traditional swiping cards when compared to the EMV chip and PIN cards which occupy 22% and this survey question covered other payment methods as well. Despite the vast variety of payment methods, the EMV chip and PIN cards only hold 22% when compared to the participants who chose traditional magnetic stripe cards comprising 36%.

The participants of the survey according to the survey report Q13 depicts that even after moving to the EMV chip cards, only 31% of the participants felt that the EMV chip and PIN cards are secure compared to the magnetic stripe cards. While 42% of the participants felt that the EMV technology is somewhat secure and the reason could be due to the poor knowledge about the security features of the EMV. This needs to be focused to improve the success of the EMV chip cards. Only 7% of the participants of the survey doubt about its security. Majority of participants are not entirely sure about its safety and raising awareness can help increase the numbers of consumers using the EMV chip cards. 20% of the participants either are not sure or do not care about the security of the chip and PIN cards to that of the magnetic stripe cards.

**What are the modes of payments used by retailers and had the EMV chip card equipment is installed in major retail stores?** Implementation of the POS devices which could read EMV cards is an important step to fully enforce the full potential of EMV standards and ensure the consumers are not affected by fraudulent activities. The survey charts Q8 and Q9 give us the picture to answer this study question. Below are the survey reports for Q8 and Q9, respectively.
By observing both the survey reports it is clear that EMV chip card POS devices are not fully enforced in the retail stores. In the survey report of Q8, only 24% of the participants responded of having the EMV chip and PIN equipped POS readers while
most of the retailers are still relying on the traditional magnetic stripe readers for accepting payment from consumers at their stores. The same is in survey report Q9 as well where only 31% of the participants responded that they are confident of EMV card readers being present and could be used for the payments. Majority of them chose Magnetic strip cards clearly stating that the EMV card reading POS devices are either not present or may not be set up for accepting payments using EMV chip and PIN cards. For EMV to be successful, the chip reading POS devices should be equipped at all retail stores and should be working to take advantage of the security of the EMV chip and PIN cards.

Did attacks reduce after shifting to EMV and are people affected even after the shift to EMV cards? Even though the move towards EMV chip and PIN cards have not been complete and are working on its implementation at full force, still there are many retailers who have not shifted to the EMV POS devices so that EMV chip cards can be used to process the payments at the store terminals. While many retailers still relying on the magnetic stripe card payment method may impose risk and have a greater chance towards fraudulent activities which could lead the consumers towards more risk of getting involved in a fraud. The survey report Q14 is very helpful in determining and answering this study question. The survey report for Q14 is as below.
Figure 35: Survey report Q14.

In this pie chart, 51% of the total respondents of the survey have reported that they have never been involved in any fraud when using the EMV chip cards and also using EMV is secure when compared to the magnetic stripe cards for payments. Thirteen percent of the respondents have reported that they have been involved in fraud more than once and 18% of the respondents reported of having involved in fraud at least once. Summing up, 31% of respondents have claimed to have been involved in the fraud which is a significant number. Due to the incorrect implementation of EMV (failure due to liability shift), poor knowledge about the security of EMV and lack of awareness in consumers on keeping the cards and data secure, all of them lead towards the failure of the security implementations of the EMV cards. Hence steps are to be taken so that the EMV system implementation takes place at full scale and all the transactions are protected and secure thereby decreasing risk to consumers due to fraud.
What is the best alternative to EMV cards and are people using it? EMV chip and PIN card technology is a secure implementation which consumers can rely on if it was implemented accurately in the USA. Liability shift played a vital role in pushing it towards failure. Though EMV standards may take time to become fully enforced, the next best alternative payment method identification is also crucial, and as the technology is growing as the time passes, there are other efficient payment methods which help in securing consumers from fraudulent activities and also process quickly when compared to EMV chip cards. The survey report Q11 is an interesting pie chart which can be used to answer this study question. Below is the survey report for Q11.

**Figure 36:** Survey report Q11.

Above survey report Q11 chart shows a significant usage of mobile payment services which are secure and process transactions significantly faster when compared to the EMV chip and PIN card payments. According to the pie chart, 62% of the participants have responded that they have used mobile payment services which
include private services like PayPal and NFC (Near Field Communication) payment services like Android Pay, Apple Pay, Samsung Pay, etc. which shows that this alternative form of payment though being new has been significantly in use at the stores for payments. Twenty-eight percent of the participants have responded that they did not use the mobile payment service and the reason could be due to the lack of knowledge. Also, this type of payments needs mobile devices or any electronic device having NFC capability to make NFC payments through their handheld or mobile devices. These payment services also have few limitations that the device used for the NFC payment has to have a battery and running for it to work while the EMV chip and PIN or the magnetic stripe cards do not need any power to work at the POS devices in the stores for making financial transactions.

**What method of shopping consumers prefer so as to identify the areas towards which focus needs to be increased?** With the growth of internet, online shopping has grown rapidly. Even retailers and third-party websites like Amazon have increased their sales by selling their products on the internet. The traditional way of shopping is to visit the retailer’s store and purchase products from the facilities. Due to technological advancement, there are several ways in which consumers are given options for purchasing items using various payment methods. To understand the interests of the consumer, survey report Q15 has a pie chart to answer this study question. Below is the survey report Q15.
Figure 37: Survey report Q15.

According to this pie chart, out of the total participants of this survey 45% of them responded to do shopping at the retail stores which mainly rely on POS devices with EMV chip and PIN card readers or the magnetic stripe cards. Even the NFC payment services are available as a method of payment at many of the retailer stores. Hence, it shows that there is an urgent need of speeding up the process of implementing EMV POS devices at retail stores so that the consumer’s data is secure and the full power of the EMV implementation can be utilized efficiently. Even the NFC payment services had increased in popularity, and many are using them which is the next reliable and secure payment method to the consumers. Steps should be taken to improve the security of NFC payment methods, its wide implementation and also is quicker and secure for payments. These features have vital importance in case if EMV fails to provide secure service. While 29% of the participants chose to utilize online shopping at retail stores and 9% of them chose to do online shopping at third party websites. Summing them
would be 38% which makes sense as they both do shopping on the internet and card details are used to process transactions at websites. Since EMV is weaker when using it for these transactions, consumers have to be very cautious and protect their data to avoid involvement in any fraud. Even the mobile payment services like Android Pay, Apple Pay, etc. are widely being used in making transactions and these services provide security and help protect the data of consumers when shopping at online stores. Awareness should increase among consumers on the risks involved in using the payment services online and should be educated on how to protect their data and have secure and quick financial transactions without risk. This survey report points out that majority of the consumers still go to the retail stores for shopping and it indicates that steps have to be taken to work on securing the correct implementation of the EMV chip and PIN cards as quick as possible.

**Conclusions**

EMV is the technical standard for performing transactions with smart cards by using the POS devices which accept them. EMV stands for Europay, MasterCard and Visa which are the three companies who had created the standard (EMV, n.d.). The EMVCo now manages the standard. The EMV technology is considered very secure and can help consumers to protect themselves against frauds. The implementation of the EMV standard in the USA is a big failure as the approach in implementing it was done using Liability shift which lead to a disaster. Big retailers felt it was a boon and started using EMV for protecting their consumer transactions from getting involved in fraud. But there are many small business owners who felt the devices are very
expensive to buy and install. According to the liability shift, if the retail stores did not upgrade to the new POS devices which are equipped to accept EMV cards by the October 1, 2015, the responsibility for any fraud at the store will be the responsibility of the store owners and not the financial institutions. This implementation has caused trouble in the shift and now at many stores even though EMV are working, there are stores in which EMV POS devices are installed but still in the process of authorization and are also many stores still using the magnetic stripe card payment method. Many threats to the EMV were discussed in the paper which could use the EMV chip cards in traditional swiping POS devices and succeeded in performing fraud. Since many retail stores are still relying on old POS devices, they need to be careful when performing transactions to avoid getting involved in fraudulent activities.

In the survey conducted for this paper, details of the EMV implementation and the preferences of consumers over the different payment methods specifically concerned to EMV chip and PIN cards are collected along with other payment forms to identify the success of the new payment technology in the perspective of the consumers. Even information is gathered to identify the alternative to the EMV which are secure and perform transactions quickly. All the data collected states that the EMV implementation was not a 100% success and many activities have to be done to implement EMV in full scale and transform the payment services to become fully secure. Many people are not aware of the EMV chip, and PIN cards and educational programs have to be conducted to raise awareness among the consumers and its security features. Even the retailers on the interest of the security of the customers
performing transactions at the stores must shift to use the new implementation of EMV to secure themselves and their customers from fraud. There is an advantage concerning to the customers in the USA as they are not held liable for the financial frauds while there are many other countries where the customers are liable in case they are affected due to fraud. Mobile payments are identified as the alternative to the EMV chip cards for payments and are very quick and secure while performing transactions. While they are quick, the mobile payments come with some limitations of requiring hardware to perform these transactions like mobile phones or any NFC enabled device.

Performing financial transactions is a necessity to the consumers in the day to day life. Such technologies must strive to keep the data of the consumers as secure as possible and should be reliable as it is used on a daily basis. Raising awareness of the technologies implemented for the consumers is very important so that they can help themselves and financial institutions to fight against fraud and make life better. Any technology developed till now is not 100% secure and foolproof but with right feedback and guidance of the users can help patch the systems and make it more secure as the time passes. The new NFC payment services are desired by the consumers as they are quick and secure. The survey also states about the increase in usage of NFC payment method and effort has to be done to build secure payment methods keeping consumer's interests in mind so that stronger payment systems are built for the future.

**Future Works**

The data collected and used for this paper through survey gives insight on the current situation and implementation of the EMV chip and PIN cards especially in the
USA. Analyzing the results of this paper highlights that steps have to be taken to speed up the process of the EMV implementation and the ways to prevent the different types of attacks on EMV cards discussed has to be implemented so that the EMV cards will be more secure. Even the paper points out to increase awareness among consumers about the security of the EMV chip and PIN cards. Lastly, it is observed that the use of mobile payment services has grown rapidly. Consumers prefer to use this as it is secure and significantly quick when compared to the EMV chip cards. Hence, more research has to be done towards the mobile payment services and NFC payment services to make it more secure and reliable.
References


Financial Fraud Action UK. (2014). *Scams and computer attacks contribute to increase in fraud, as total card spending rises*. Press Release.


Appendix

A. Survey Questionnaire

Below is the list of questions used for survey.

Section 1

EMV chip cards survey

Q1) What is your gender?

- Female
- Male
- Prefer not to say
- Other

Q2) Which age group best suits you?

- Under 15 years
- 15 - 24 years
- 25 - 45 years
- 46 years or older

Q3) What is the highest degree or level of school you have completed?

- No schooling completed
- High school graduate
• Associate degree
• Bachelor’s degree
• Master’s degree
• Doctorate degree

Q4) What is your employment status?
• Employed for wages
• Self - employed
• Out of work and looking for work
• Out of work but currently not looking for work
• A homemaker
• A student
• Unable to work
• Prefer not to say

Q5) Have you ever heard of the EMV chip cards?
• Yes
• No
• Maybe
Q6) Did you receive cards with chip from all the financial institutions you are associated with?

- Yes
- No
- Maybe

Section 2 - Modes of payment and preferences

Q7) Please check all the modes of payment you heard of

- EMV Chip cards
- Traditional swiping of the card for payment
- Mobile Payments using private services like PayPal etc.
- NFC payment services like Android Pay, Samsung Pay etc.
- Crypto currency

Q8) What kind of payment options do you find at most of the retailers you visit and are working?

- EMV chip cards
- Traditional POS machines accepting card swipes
- NFC payments (E.g. Android Pay, Samsung Pay, Apple Pay etc.)
- Only Cash
Q9) Which payment method you are most likely expecting to pay with and confident about it working at any retail store?

- EMV chip cards
- Magnetic stripe cards
- Mobile payments
- Not sure

Q10) Are you comfortable with the time taken at checkouts using the Chip cards over traditional swiping method?

- Yes
- No
- Maybe

Q11) Did you ever use mobile payment services like Android pay, Samsung pay or PayPal for your daily expenses?

- Yes
- No
- Maybe
Q12) What forms of payment you prefer for day to day payments? (E.g. gas, groceries etc.)
   - EMV cards
   - Swipe cards
   - Mobile Payments using third party services like PayPal
   - NFC Payment Services like Android Pay etc.
   - Cannot say

Q13) How secure do you feel about using the Chip cards over traditional stripe cards?
   - Very secure
   - Somewhat secure
   - Not sure, does not matter
   - I doubt about security of the chip cards

Q14) Have you ever been involved or affected due to frauds in chip credit cards?
   - Yes, more than once
   - Yes, at least once
   - Not sure
   - No
Q15) If you prefer to do shopping. What method do you prefer?

- Shopping at the retail stores
- Online shopping in retailer’s website
- Shopping in third party websites
- Not sure