A Survey on Contactless Smart Cards and Payment System:

Technologies, Policies, Attacks and Countermeasures

Brij B. Gupta, Department of Computer Engineering, National Institute of Technology, Kurukshetra, India & Department of Computer Science and Information Engineering, Asia University, Taiwan

Shaifali Narayan, National Institute of Technology, Kurukshetra, India

ABSTRACT

In recent years, contactless transactions have risen rapidly. It includes NFC, MST, contactless cards, and many other payment methods. These payment methods have certain security issues, and attackers are in a regular search for the exploits to break its security. These security issues require proper analysis to secure user data from attackers. This article will discuss the contactless smart cards and payment systems in detail including the techniques used for securing user data and different possible attacks on the technology used for communication. The article also presents some countermeasures to prevent the attack and issues with those countermeasures. In addition, the article includes some future research issues and suggestions to overcome the security issues in contactless payment system.

KEYWORDS

Applications, Contactless, Magnetic Secure Transmission, Near-Field-Communication, Smartcards, Tokenization

1. INTRODUCTION

With the expeditious growth in smart cards and payment technology in today's time, human life has become much easier and smart driven. Smart cards are the small plastic cards with chip embedded to them along with CPU, RAM and ROM for processing and storage (Rankl & Effing, 2004). According to a report, the smart card market will grow at 8.7% Compound Annual Growth Rate (CAGR) by 2023 (Report Buyer, 2018). There are many entities involved in smartcards, such as card holder, terminal, data owner, card manufacturer, card issuer and software manufacturer (Schneier & Shostack, 1999). Smart cards have been used to identify users and can also be used for logical and physical access as they are the cost effective multi-function cards (Taherdoost et al., 2011). With the ease provided by smart cards, they are now broadly used from secure payment applications like credit and debit cards, public transport system (Markantonakis et al., 2008) to user identification and authentication applications like smart health cards (Aubert & Hamel, 2001; Hsu et al., 2011), employee cards (Chen, 2016), membership cards (Conlon & Whitacre, 2005), IoT (Vanderhoof, 2017; Gupta & Quamara,

DOI: 10.4018/JGIM.2020100108

2018); mobile based applications as Subscriber Identity Module(SIM) card for making paid television connections, purchasing goods, etc. For the smart card-based applications, to control the access dynamic security policies were proposed (Gupta & Quamara, 2018b).

Smart cards are frequently used in applications that require strong authentication and security protection in comparison to other machine-readable data storage techniques like bar- code and magnetic-stripe. The self-containment property makes them impervious to attack as they don't rely upon the potentially vulnerable external resources. Smart card offers vital system safety modules that are needed for nearly any form of network information exchange (Smart Card Basics, 2018). Smart cards protect against security threats from negligent storage of user password to sophisticated system hacks. There have also been some suggested schemes that use user biometrics such as face recognition (Parmar & Mehta, 2014), iris matching (Nedjah et al., 2017), fingerprint matching (Nedjah et al., 2017b) for user data security. The main driving factor in the success of smart card is its ability to perform security sensitive operations and maintain the integrity of the data stored in the card. For example, the cost to control password reset in an organization is very high, but in such an environment smart cards are a cost-effective solution. However, in terms of storage and computing capacity, their resources are obligatory. Also, for power supply and clock mechanism card depend on the card readers (Moore et al., 2002). With the increase in the number of its application, several opportunities have been generated for the attackers to extricate the secret information (Messerges et al., 2002).

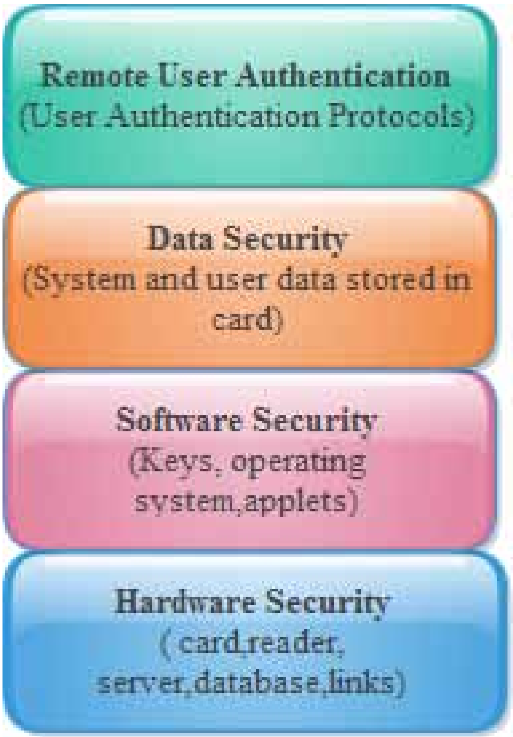
The major contribution of smart cards is in the banking sector. Around the world, bank-controlled co-ops (American express, MasterCard, Discover, VISA) have generated millions of smart cards under the Europay, MasterCard, VISA standards (EMV). The chip and pin card like credit card, debit card is commonly used for bank issuance in many countries. The security of data is insured by the two-factor authentication which also eliminates the Man in the middle and Trojan horse which replay a username and passwords. Using smart cards has also decreased costs, as transactions are managed by the client and do not involve a bank employees and paperwork time.

While developing a smart card security concerns are specific to card microprocessor, operating system, and software platform, which can be achieved by a multi-level security model (Gupta & Quamara, n.d.). Multi-level security model as described in Figure 1, includes hardware security, software security, data security and the remote user authentication. The hardware security mainly includes security of smart cards, readers, communication links, servers and the storage devices like database. Software security which is mainly concerned with the security of the applets, cryptographic keys, and the system software. Data security focuses on the security of the user and system specific data stored in the card to carry out the user operation. Remote user authentication security involves prevention against the attacks such as session key disclosure attack, stolen smart card attack, and brute force attack (Gupta, 2018; Almomani et al., 2013; Jiang et al., 2018; Li et al., 2019). Authentication systems were created in the initial phases of communication for remote user and server authentication.

Contact and contactless smartcards are frequently smartcards in different application areas. Contact smartcard being prone to skimming (Bond et al., 2014) and side channel attack (Kasper et al., 2009), were replaced by the contactless smartcards. The card allows a user to pay through a safe radio interface. Being quick and simple, these cards are also susceptible to cloning a side channel attack (Roland & Langer, 2013). These attacks occur at interface level and at data reader. Safe systems should be developed to protect cards and user information from attack and data theft.

Rest of the paper is organized as follows. Section 2 will cover the history of smartcards and some of the major global achievements that are associated with the growth of smart cards, global industrial statistics and fraud statistics, and motivation. Section 3 covers the type of smart cards based on various parameters. Section 4 will give the overview of contactless payment system which will include working of contactless smartcards and payment terminal. In addition, it will also cover tokenization including cryptogram and key management techniques. Section 5 covers the contactless payment technology including possible attacks and their countermeasures. Section 6 covers the open source

Figure 1. Multi-layer security for smart card-based applications


Remote User Authentication
(User Authentication Protocols)
Data Security
(System and user data stored in card)
Software Security
(Keys, operating system,applets)
Hardware Security
(card,reader, server,database,links)

tools that are available for development and management of smart cards-based applications. Section 7 discusses some of the practical applications accepted world-wide for contactless payment system. Section 8 discusses the future research issues and Section 9 outlines the future scope and conclusion.

2. EVALUATION OF SMARTCARDS, STATISTICS AND MOTIVATION

2.1. Global Study of Smart Cards

With the increase in the applications of smart card globally, we need to focus more on research to identify new challenges by increasing the number of new security attacks and developing secure models. The development of smart cards was initiated in early 70's in Japan, France and Germany (Shelfer & Procaccino, 2002). Concept of smart card was given in 1968 and 1969 when two German engineers filed a joint patent for the chip card, which consist of a plastic body with a microchip embedded into it. And in the next few years, numbers of ideas were presented related to its use and applications across the globe and many commercial manufacturers started working on it collaboratively for its development. Prime events related to the evaluation of smart cards are outlined in Table 1.

2.2. Global Information and Industrial Statistics

Based on a study on "Smart card market by Communication, Components, Applications, and Geography – Global forecast to 2023" by 2023 the market is supposed to reach USD 21.57 billion from USD 14.22 in 2018 with CAGR of 8.7% between 2018 and 2023. The use of smart cards in Banking Financial services and Insurance (BFSI) has risen, with the shift from magnetic card to EMV cards. 63.7% of transactions around the globe are EMV and 54.6% of cards issued are EMV cards (EMVCo, 2018). As per Reserve Bank of India's annual report, digital payments were 1.2 times higher than the

Table 1. Evaluation of Smart Cards

Year	Description
1968	Two German engineers and inventors filed a joint patent for the automated cards.
1970	Dr. Kunitaka Arimura of Japan filed the first and only patent on the smart card concept.
1974	Roland Moreno of France filed the original patent for IC cards, which was later labelled as smart cards.
1977	Commercial manufacturers Bull CP8, SGS Thomson, and Schlumberger began developing IC cards.
1979	Motorola developed the first secure single chip microcontroller for use in French banking.
1982	The world's first major IC card testing in France.
1984	Field trials for ATM bank cards with chip were successfully conducted.
1987	First large-scale smart card application implemented in the United States with the U.S. Department of Agriculture's nationwide Peanut Marketing Card. Smart card-based drivers were license in Turkey.
1991	First Electronic Benefits Transfer (EBT) smart card project launched for the Wyoming Special Supplemental Nutrition Program for Women, Infants, and Children (WIC).
1992	A nationwide prepaid (electronic purse) card project (DANMONT) was started in Denmark.
1993	Field test of multi-function smart card applications in Rennes, France, where the Telecarte function (for public phones) was enabled in a Smart Bank Card.
1994	EMV published joint specifications for global microchip-based bank cards (smart cards). Germany began issuance of 80 million serial memory chip cards as citizen health cards.
1995	Over 3 million digital mobile phone subscribers worldwide begin initiating and billing calls with smart cards.
1996	Over 1.5 million VISA Cash stored value cards were issued at the Atlanta Olympics.
1999	GlobalPlatform, a non-profit organization that creates and publishes specifications for secure chip technology, was founded.
2001	GlobalPlatform Card Specification v2.1 was published.
2005	EMV compliant cards introduced in Malaysia
2006	Contactless payment system infrastructure in the US was introduced.
2007	first contactless cards in the UK were issued by Barclaycard
2009	First large-scale Public Key Infrastructure (PKI)–based smart card management systems were deployed.
2014	Master card became first company to accept EMV cards in United States. Also, Apple introduced ApplePay (Burge, 2015), a mobile payment and digital wallet service which works on Near Field Communication that allows users to make payments in person, in iOS apps, and on the web
2015	Samsung introduced SamsungPay, a mobile payment service working on Near Field Communication (NFC) and Magnetic Secure Transmission (MST).
2016	Erste Group launched an NFC only debit card implemented as a sticker in Austria
2017	Served us an exciting prelude for the biometric smart cards market.
2018	Financial services giant aimed for a commercial rollout of biometric payment cards

number of debit card transaction in 2018-2019. Table 2 represent the latest statistics from American Express, Discover, JCB, Mastercard, UnionPay, and Visa, as reported by their member financial institutions globally (EMVCo, 2018b). The growth in smart card market is due to the increase in the online payment method which allows user to make secure and reliable payments. As per the Nilson report (2018), in the next five years the global brand cards will increase by 3.86billion.

With research in the path of going contactless, the next achievement was the secure element. A secure element is a microprocessor chip that enables sensitive information to be stored and safe

Table 2. Worldwide EMV chip card deployment and adoption

	2015		2016		2017	
Region	**EMV card**	**Adoption Rate**	**EMV card**	**Adoption Rate**	**EMV card**	**Adoption Rate**
Africa & Middle East	160M	61.2%	184M	68.7%	219M	74.8%
Asia Pacific	2459M	32.7%	3331M	38.8%	4147M	45.7%
Canada, Latin America and Caribbean	680M	71.7%	717M	75.7%	820M	85.7%
Europe Zone 1	881M	84.3%	921M	84.9%	939M	84.4%
Europe Zone 2	200M	52.3%	243M	63.7%	276M	71.4%
United States	394M	26.4%	675M	52.2%	785M	58.5%

applications like payment apps to be run. Eurosmart members manufacture and personalize secure elements along with software and infrastructure around it. The secure element shipped in 2016 was 2.9 billion while that in 2017 was 3 billion. The contactless secure element market was increased by 1.9 billion in 2017 while 2.1 billion contactless secure elements were predicted to be shipped in 2018. The figures below are divided into following main areas – Telecom, device manufacturer, government and healthcare, payment and banking, transport, pay television and others. Table 3 describes the worldwide secure element forecast while Table 4 describes the worldwide forecast of contactless secure elements. Table 5 describes the forecast of Near Field Communication SIM along with embedded secure element.

Table 3. Worldwide secure element forecast-2016-2018(millions of units)

	2016	**2017**	**2018 forecast**	**2017 vs. 2016 growth**	**2018 vs. 2017 growth**
Telecom*	5450	5600	5600	2.75%	0.00%
Financial services	2900	3000	3150	3.45%	5%
Government – Healthcare	460	485	510	5.43%	5.15%
Device manufacturers**	330	400	470	21.21%	17.50%
Transport	260	280	300	7.69%	7.14%
Pay TV	120	100	95	-16.67%	-5%
Others***	90	90	90	0%	0%
Total	9610	9955	10215	3.59%	2.61%

*Secure elements with a SIM application

**Device manufacturers represent embedded secure elements without SIM

***Others include logical and physical access

2.3. Global Contactless Payment Card Fraud Statistics

According to a portal, latest figures form US indicates that the contactless card fraud overtook cheque fraud in the first half of 2017, hitting 5.6 million Pounds. As per the UK Finance 2017 annual report (UK Finance, 2018), card fraud loss in 2017 amounts to 24.2 million Pounds, lower than in 2016

Table 4. Worldwide contactless element forecast-2016-2018(millions of units)

	2016	2017	2018 forecast	2017vs2016 growth	2018vs2017 growth
Financial services	1300	1400	1500	7.69%	7.14%
Government-healthcare	270	285	300	5.56%	5.26%
Transport	260	280	300	7.69%	7.14%
Total	1830	1965	2100	3.42%	6.87%

NFC SIM along with embedded secure element includes NFC UICC secure element; embedded secure element and embedded UICC.

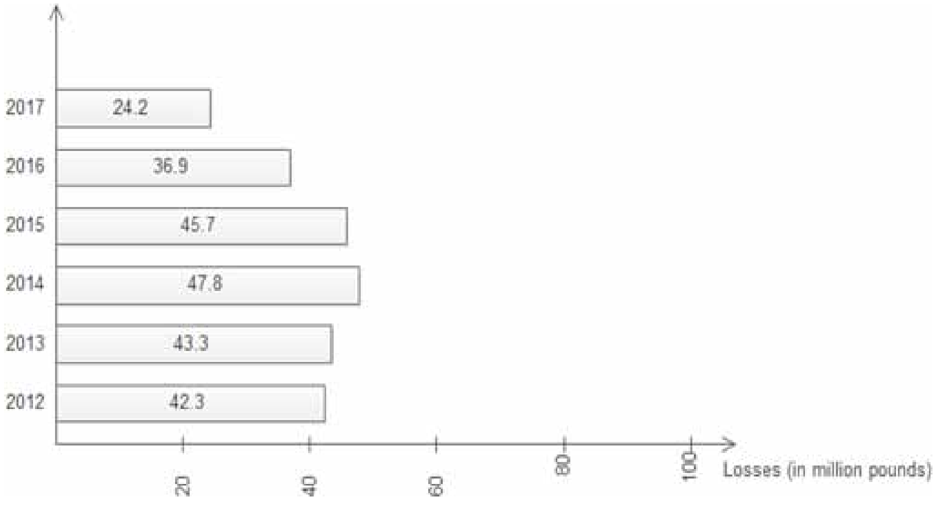
Table 5. Worldwide NFC SIM+ embedded secure element (millions of units)

	2016	2017	2018 forecast	2017vs2016 growth	2018vs2017 growth
NFC SIM+ embedded secure element	500	548	620	9.60%	13.14%

which was 36.9 million Pounds in the UK. The fraudster utilized compromised magnetic stripe card information for such kind of attack. Mobile banking fraud lost approximately 5.7 million Pounds in 2016 and 6.3 million Pounds in 2017. Figure 2 demonstrates the losses due to fake card frauds.

According to national reporting centre for fraud and cybercrime, there were 2739 reports of contactless fraud in 2018, which totals to £1.18 million — up from 1,440 cases worth £711,000 in the same period in 2017 (standard, 2019). According to a research, the frauds were due to cloning of card details through low tech methods, which included distraction thefts and cash machine "entrapment devices". The criminals can use rogue card readers and smartphone merely by brushing past the owner to read cards. According to the UKF fraud statistics, in the first half of 2018, the real percentage of all

Figure 2. Counterfeit card fraud in UK (According to UK 2017 annual report)



card fraud losses by value resulting from contactless fraud was 3%. According to researchers at the security firm Positive Technologies, a newly discovered vulnerability in Visa's contactless payment cards might allow fraudsters to bypass the payment limit of £ 30 ($37) at several U.K.- based banks (Bankinfosecurity, 2019). The researchers, though, restricted their studies to U.K. Banks seem to be exploiting the vulnerability in other nations as well, scientists clarify in a blog. The researchers told Forbes that by using the proxy device and the man-in - the-middle attack they were able to make payment of up to £ 101.

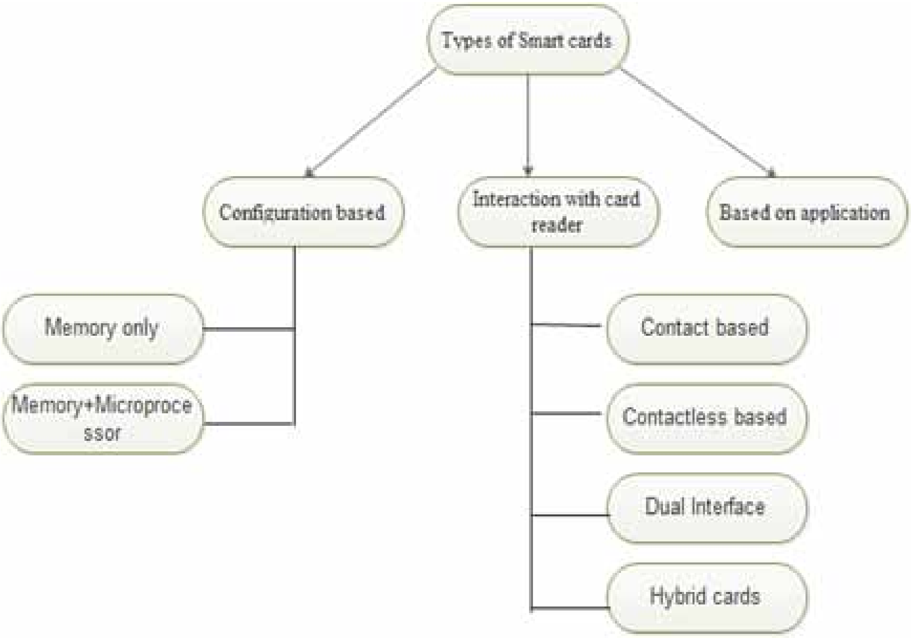
2.4. Motivation

Digital payment techniques have had an incredible rate of acceptance in consumer devices around the globe over the past few years. Many large companies are adding support for NFC (Near Field Communication) and MST (Magnetic Secure Transmission) to all kinds of devices to enable consumers to make monetary transactions. Some of these businesses protect themselves as part of the payment technology by applying tokenization. And it is well known that simple mechanisms can be used to bypass these techniques. With all these changes in the NFC ecosystem, the field of information security is not well prepared to protect against growing new attacks in this area. Relay and replay attacks in the payment industry are more prevalent than ever, becoming more complex and sophisticated by the day. In contactless payment, to reduce the flaws, a simplified and effective model is needed. Methods and models must be developed to ensure the card data security from cloning and frauds.

3. TYPES OF SMART CARD

Based on the chip used for the operation and operations that can be performed on the data stored in the card, smartcards can be divided into different categories. Using a card in an application depends on various card factors, such as- nature of application, security demand, purpose of the card, etc. Figure 3 defines kinds of card based on setup, card reader interaction and their use in different applications.

Figure 3. Types of smart cards



3.1. Configuration Based

Configuration-based cards can be distinguished based on the parts in the card used to process the card information. Based on the setup, there are two kinds of cards– memory-based cards and memory and microprocessor cards.

Memory based cards are the cards that must conduct a fixed function and has a limited functionality. These cards do not have any processing power and it is not possible to manage the information stored in the card. The addresses in the card are fix, where the information in the card can be written and initialized only once. For example - prepaid phone card (Lorsch, 1999). Such cards have no security mechanism for the stored data, so encrypted information is stored in the card. On the other hand, there are also rewritable memory cards that can be manipulated by a card reader but cannot manage their data. For example, card-based hotel room keys.

Memory and microprocessor cards are the one that consists of a microprocessor to process and manage the card's information. It has an operating system, for managing hardware and software resources and providing the services required. It is made up of memory unit– RAM, ROM and EEPRO. ROM is used to store the operating system, RAM is needed to perform quick computation and process results, and EEPROM is the area where the code is written to perform the application-related operation. The power and clock are supplied to the card when card waved at the card reader. For example, the metro cards (Barry et al., 2002).

3.2. Interaction with Card Reader

Based on the sort of contact with the card reader, the cards can be split into four kinds- contact, contactless, hybrid and dual interface. Each of the type is discussed below.

Contact based card are the cards where card's exterior surface connects to the reader when inserting a card. In magnetic stripe cards, the card is swiped on the reader for data transfer (Infosino, 2004). Most of these cards are used in banking sector, in the form of ATM card, credit card or debit card (Yang & Ching, 2013). With the assistance of cloning device that is readily accessible on the market, magnetic swipe cards were readily accessible to clone (Masters & Turner, 2007). This leads to chip-based contact cards being developed. In chip-based cards, the reader pins come into touch with the chip present on the card, the power and clock supply causes communication. Chip based cards are considered safer than magnetic stripe cards.

Contactless smart cards have an integrated circuit that can store information and use radio frequency to communicate with the terminal (Halope & Zupanek, 2004; Andersson, 2016). For example, bank cards, transit tickets, etc. Contactless cards were first used in 1955 in electronic ticketing in South Korea. The Radio Frequency Identification (RFID) is primarily used by the contactless smart card reader to read, write or interact with the card (Paret, 2005). To make payment fast and easy, multiple banks support contactless cards (Alliance, 2007). The proximity cards have a limited memory and can either be memory based or microprocessor based. The RFID card tends to be effectively cloned with the cloning machines and need a legitimate security component from getting cloned.

Dual Interface cards which support more than one technique of reading the data from the cards (Lee & Kwan, 2005). Proper key management approaches are needed to secure user data from key stolen attacks (Habraken, 2014). Most of the payment cards utilized now days are built with magnetic strip, embedded chip and sometimes with RFID mode (Finn et al., 2015). Such cards can be used as contact cards or contactless cards depending upon the terminal in use (Kreft, 1998).

Hybrid Cards supports both the contact and contactless interface embedded in one single card. They are installed with separate chip for each of the interface which is not associated with each other (Fidalgo, 1997). The processor of these cards cannot be simultaneously updated. Hybrid cards are the multifunction cards, where a single card can be used in multiple transactions (Jean & Lecomte, 2001). For example, for pupil and student ID cards, RFID cards can store money related values for canteen and can provide access to areas like library.

3.3. Based on Application

Cryptographic cards are used for secure identification and storing digital signature and uses RSA algorithm and Digital Signature algorithm for securing the information (Naccache & M'Raihi, 1996; Li et al., 2018). Credit and debit cards are issued by the banks which provide an easy way to the users to purchase the items without carrying the cash (Cuervo, 2001). Travel money cards (Canstar, 2018) are the specially designed debit cards to securely buy foreign currencies and take it overseas. Loyalty cards (Rowley, 2000) are given by the retailers to their customers, which contain the information about reward points or the discount given to customer. Smart cards are also used as security token in computer systems (Clark, 1995). The web browser uses smart card to store the certificates and can later be used for a safe web browsing. MyKad is a multi-function card issued by the Malaysian government to be used for identification, travel documents, e-wallet, health information of user, driving license, ATM card and many other features (Noorhuzaimi et al., 2008).

4. CONTACTLESS PAYMENT SYSTEM AND ITS MANAGEMENT

Contactless cards can be used in other sectors replacing contact cards, for easy and fast use of application. Communication with the terminal in contactless cards is via NFC through a card-built antenna (Abrial et al., 2001). The contactless smart card and its reader follows the international standard, ISO/IEC 7816, ISO/IEC 14443, and can also implement a variety of cryptographic protocols like RSA, AES, ECC, and 3DES (Lacmanovic et al., 2010). Contactless smart card differs from RFID tags in terms of memory, security, privacy, application area and read range (Nath et al., 2006; Juels, 2006). The range is about 10 cm for contactless cards while the range for RFID tags is one meter, which is much higher than contactless cards. Multiple payment system cards such as Mastercard, Visa, Rupay, etc., support contactless payment. The user can perform unlimited transactions in a single day with the contactless cards. Some range of transactions can be performed without pin and does not provide any method to authenticate the user. It is a disadvantage of such cards which lead to many losses due to fraud transactions. To overcome such fraud transactions, payment process needs improvement in terms of user authentication and confidentiality.

Further, in this section we have discussed working of contactless smart cards, mobile terminals for contactless application, concept of tokenization, NFC and MST based technology and different attacks possible on them and their countermeasures.

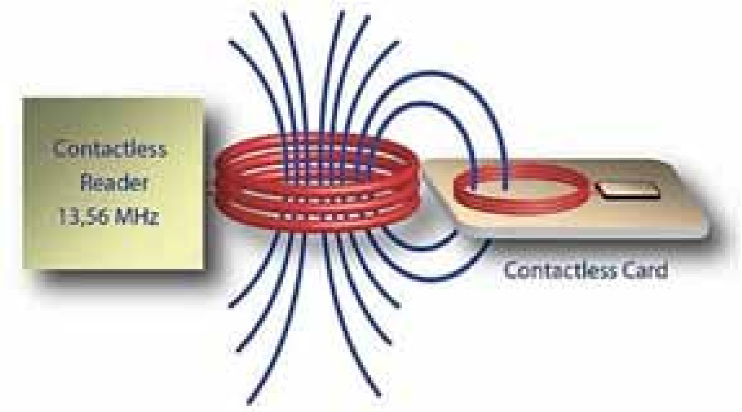
4.1. Working of Contactless Smart Card

The contactless card can be in active or passive state at any time (Pampattiwar, 2012). The active state is the state when the information is transferred to the card reader from the card, whereas the passive state is the state when the card is not in use. The reader transmits an electromagnetic radio field around it to build communication. The card primarily includes a chip attached to the coil to receive power from antenna. When a passive card contacts with the field, the antenna captures the signal to generate power and supply it to coil (Coskun, et al., 2013). The card turns active and performs terminal authentication to transfer data (Coskun et al., 2015). The power supply stops when the user removes his card from the terminal and card shifts from active state to passive state. Figure 4 shows the connection between the chip and the coil in a smart card.

4.2. Contactless Payment Terminals

Contactless payment terminals are the terminals where user can use NFC or MST to make a transaction through smartphone or contactless card. According to (Wang et al., 2016), following are the types of the terminal where the mobile payment can be performed.

Figure 4. Connection of coil and chip in contactless card Source: edn.com (2019)



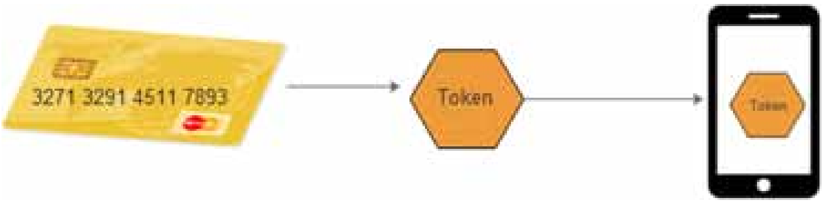
1. Payment at the POS: - It enables a client to pay at the POS with their mobile phone. The smart phone functions as POS terminal smartcard that causes payment. For example: - ApplePay and SamsungPay. The built-in payment method is easy to setup on a mobile device. There are different phases involved – registration phase, validation phase, authentication phase. The NFC and MST are two technologies used for such payment.
2. Mobile as the POS- This payment scheme allows the merchant to use the mobile phone as a POS terminal to perform the transaction of the card. For example: Square reader that is attached to a mobile device to perform transaction from credit card reader and keyed-in transaction. Three types of card reader supported currently- square reader for magnetic stripe cards, square reader for EMV chips, and square contactless and chip reader which accepts NFC payments.
3. Mobile Payment Platform- This method enables online payment services on a mobile device by downloading and installing application on a mobile device. This method can also act as payment at POS and requires bank account or the card account to be linked to the mobile payment account. Example - PayPal.
4. Independent System- It provides the similar payment services as the mobile payment platform. Independent mobile payment services are the one where the company creates their own payment platforms for the user ease. For example, AmazonPay. Mobile payment platform differs from independent mobile payment system in a way that mobile payment platform can be used by other companies and online sites for making payments while the independent mobile system is used by the company itself.
5. Direct carrier billing – This method allows users to buy products through mobile devices where payment is not made by any debit or credit card but is charged in the mobile subscriber phone bill. It usually involves charging through SMS. For example, Boku, popular in Europe.

4.3. Tokenization

Tokenization is the process where the credit card essentials like card number, CVV number etc are replaced by a substitute value which is called as the token Primary Account Number or digitized(PAN) (Ornce et al., 2012; Samsung Pay, 2018). The technique is used by a non-merchant organisation to generate, store and provide the token to a merchant, which can be used to perform a transaction (Gaspar, 2015). The token is used to protect the real card number values from misuse and theft. To make the information more secure, cryptogram is also used (Brown & Chatelain, 2008). Cryptogram consists of the unique authentication data which is generated by the mobile and demonstrates to the card network that the device and the card in use are genuine and not a vehicle for intercepted or cloned credentials. The token can be mapped back by the Token Service Providers (TSP) which are maintained on highly secure servers (Royyuru, 2013). Global payment network offer tokenization facilities, which are accessible to all members of the card association. TSP can be supported by a third party and can also be owned separately by card issuers themselves. Account verification and authorization of the cardholder during the token request period secure the cardholder data from attacks and leakage (Stapleton & Poore, 2011).

For token request and issuance, the mobile wallet provider-like SamsungPay and ApplePay must be registered with the card issuer's TSP. When the user enrolls his card, the Token Requester (TR) sends a token request on behalf of the cardholder and the device. The TSP on receiving the request follows the identification and the verification process with the card issuer through payment network. The token PAN is linked to the Funding Primary Account Number (FPAN) and not the card number printed on the plastic card. The token is active if the account is active even if the account is cancelled or if the plastic card expires. When the card is lost, the new issued FPAN is linked to the existing DPAN (Figure 5).

Figure 5. Tokenization Process



4.3.1. Cryptogram

Cryptogram is encrypted data derived from the DPAN, Application transaction Counter (ATC), and timestamp which prevent replay attack and ensures transaction integrity. Cryptogram is produced using cryptographic key based on the card network algorithm. The key is stored in the trusted zone of the device and can be static or dynamic depending on the card network. Static cryptographic keys are used over a long period of time and for multiple key exchanges, while the dynamic keys are generated for each exchange. Multiple dynamic keys also known as limited use keys are provisioned at card enrolment. The number of keys provisioned is regulated by the payment network. Each time a transaction is made the key is consumed and replenished according to the card network replenishment logic. The card network holds the master key to their card product and use it to generate a unique derived key (UDK) for each cardholder. Once the cryptogram is generated using the static/dynamic keys in the device, it is then verified by the TSP on behalf of the issuer, transaction processing continues. When the keys are expired, the device must be online for fresh transaction keys.

4.3.2. Key Management

Tokens and keys are stored in an encrypted form in the Trusted Execution environment (TEE) using a device specific hardware-based key. There are two key management methods for token replenishment – cloud based (Chandramouli et al., 2014) and TEE based (Jawale & Park, 2018).

In cloud based key management, the dynamic keys are stored in device's TEE and there are some fixed dynamic numbers of keys for an enrolled card. When the keys are consumed, they are replenished by the TSP based on - the number of keys remaining, already used, and time to live. If all the available keys are consumed, the transactions cannot be carried out. When the device comes back online, connectivity is restored, keys are replenished and normal transaction processing resumes. The TEE based key management models the static key which are used for multiple transaction. The static key is stored in the TEE and cryptograms are generated on demand. It allows the user to make purchases whether the device is online or offline and does not require key replenishment.

5. CONTACTLESS PAYMENT TECHNOLOGY

NFC and MST are two popular technologies that are used for contactless payments. It does not require the mobile device to interact physically with the terminal of a merchant. The technology works on physical proximity with the merchant device. Discussed below is the survey of two technologies which includes their description, possible attacks and proposed solutions to prevent the attacks.

5.1. Near Field Communication

NFC is a short-range wireless communication technology which facilitates mobile phone to communicate in a short range. Philips and Sony jointly developed NFC for contactless communication in 2002. It is a half-duplex communication protocol for providing communication between the devices. NFC and RFID works on same mechanization, but NFC is customized to mobile devices and works on 13.56 MHz while RFID works on a larger range and is known for tagging of customer products. NFC is used for many purposes like file transfer, conducting payment, NFC tags and many more. NFC works on different communication modes which are further described in the next section.

5.1.1. Modes of communication

There are different modes of using NFC with the other device. The selection of the mode is done based on the purpose for which NFC is taken into use. The different modes of NFC are-

1. Reader-Writer mode
2. Card emulation
3. Peer-to-peer mode

Reader-Writer mode of NFC allows a mobile device with enabled NFC to communicate with the NFC tags. This mode is based on the digital aspects of ISO/IEC 18092 and ISO/IEC 14443 for digital protocol. NFC mobile is capable of reading NFC forum mandated tag types which are Type 1, Type 2, Type 3, Type 4. With the help of NFC tags user can fetch the required information stored in the tag and take the necessary action later. For example- NFC tags can be used for storing the Wi-Fi passwords, or for storing some necessary URL. Tags can be locked by the owner so that its content cannot be modified by somebody.

Card Emulation Mode allows an NFC enabled device to function like a contactless smartcard and execute transactions with just a single touch (Roland, 2012; Alattar & Achemlal, 2014). It is based on the digital aspects of ISO/IEC 14443 for the digital protocol. The NFC enabled device communicates with the card reader in the same way as the traditional contactless smartcard. Biometrics and pin are used as authentication technique. In the communication process, NFC reader communicates with the application which is stored in the Secure Element (SE). SE is the microprocessor chips which are used to store sensitive data and to run the applications securely. The card emulation mode uses SE for functions that need high security. There are three ways to implement the SE:

- *In the SIM*: This has the advantage of portability and is the preferred approach in GSM countries. Using a special purpose SIM is the drawback of the method.
- *Embedded SE component*: It is a separate chipset in the handset. It is convenient for handset manufacturers for quick implementation. Handset and OS manufacturers rule the access to the SE which is a drawback.

- *A removal SE component*: This approach is used to create a removable separate chipset in the handset and often implemented as a SD card. The drawback is that special hardware needs to be used by the user.

Peer-to-Peer mode of NFC allows the two NFC enabled device for a bidirectional communication. The two devices can exchange the files, data, etc. It is standardized to ISO/IEC 18092 as NFCIP-1 and enables the "request- response model" between the two active devices. It provides segmentation and reassembly capability, ordered data flow, data flow control, and error handling by using accept (ACK) and reject (NACK) frame. The communication is performed in the link layer which makes it more error free and reliable.

5.1.2. Possible Attacks in NFC

NFC is a technology which helps in providing contactless communication between the user device and the terminal. Communication is required to be secure and prevent the user data from leakage and misuse. The attacks that affects the NFC communication most are listed below: -

1. Eavesdropping

Eavesdropping is a problem in NFC communication because it is wireless. It is claimed that the victim's NFC communication can be scanned for up to 10 meters (Haselsteinr & Breitfuß). The device used to conduct the audit is a transmitter unit consisting of a powerful antenna capable of capturing the signals from a distance (Kortvedt & Mjolsnes, 2009). It is difficult to detect the eavesdropping attack at the victim side, so it is required to take the necessary countermeasures. To prevent the attack, communication channel between the devices is secured by encryption. Also, tokenization is used to secure the user data from such attacks.

2. Relay Attack

Relay and replay attacks in the payment sector are more common than ever, becoming more complicated and sophisticated by the day. Since NFC signals can be captured when proper equipment is used, the relay attack can be carried out (Hancke, 2005; Francis et al., 2010). According to Chothia et al., (2015), it is possible to relay the signals from Mastercard, payWave, and PayPass bank card by making use of NFC based smart phones. Even if the cards are in the user wallet, the attack can be carried out. NFC based smart phones can also be used in relay attack to capture the signals (Francis et al., 2013). Lowering the time out could be a counter to relay attack along with proper authentication. Also, binding the token to a device can also lower the relay attack.

3. Skimming attack

In contactless payment cards, skimming attack is possible even without having any physical access to the card. Skimming contactless cards can be done when the NFC-based cards comes into contact with an active NFC device and the shared information cloned in another card by the attacker (Heydt-Benjamin, 2007). Also, it is possible to extract the static data from chip-based credit cards and later encode the information in a magnetic stripe-based card. To counter the skimming attack, it is necessary that the information stored in the card cannot be accessed without permissions (Bond, 2014). There are other attacks that are feasible with NFC communication besides these attacks. Example- data manipulation where the attacker intercepts and alters the data during the transmission (Haselsteiner & Breitfuß, 2006). Data destruction where the attacker blocks the transmitted data so that the recipient can't intercept it (Fahrianto et al., 2016). Many schemes have been proposed to prevent the attacks in NFC and are discussed in the next section.

5.1.3. Schemes Proposed as Countermeasure

To prevent the various attacks in NFC, schemes and methods were built by using different parameters. For proper user authentication and securing user data, the schemes and methods were proposed (Table 6).

Table 6. Schemes proposed to prevent attack on NFC payment system

Author	Description	Advantage	Drawback
Chen et al. (2010a, 2010b)	● Uses GSM primitives ● Combines existing 3G cryptographic primitive and algorithms with SIM identification and authentication	● Provide security to low value payment and customer anonymity	● Scheme works online and depends on the communication channel. ● The scheme is limited due to the use of the T M SI for original user identification.
Lee et al. (2013)	● Uses mobile device for authentication and as an authentication medium along with an authentication center. ● Uses symmetric and asymmetric cryptography along with hash function.	● Prevents replay attack and man-in-the-middle attack.	● Lacks mutual authentication, message authentication and recipient authentication.
Ceipidor et al. (2012)	● Protocol provides mutual authentication between the NFC phone and the POS terminal to share the session key, achieved by using trusted third-party authentication server.	● Protocol provides message authentication, mutual authentication and confidentiality.	● Protocol lacks message integrity and prone to brute force attack due to static keys.
Leon-Coca et al (2013)	● Protocol for authenticating Spanish ID cards and wireless NFC devices. ● Protocol was based on the RSA encryption and DES session.	● The scheme satisfies confidentiality, non-repudiation and message authentication.	● Lacks mutual authentication message integration. ● Prone to brute force attack.
Thammarat et al. (2015)	● Introduced two new mutual authentication protocols. ● NFCAuthv1 is used to provide authentication between the NFC device and the authentication server ● NFCAuthv2 is used to provide authentication between the NFC device and authentication server through a POS terminal. ● Protocols are based on the symmetric key cryptography and limited use of session keys and its distribution.	● Protocol provides partial mutual authentication.	● Lacks in achieving NFC mobile anonymity, defeating tracking and desynchronization attack. ● Key forward and backward secrecy is not satisfied
Nashwan (2017)	● Secure authentication protocol to provide strong security to the NFC based mobile payment systems.	● Secure against replay attack, tracking attack, impersonate attack, and desynchronization attack.	● Performance is analyzed under certain assumptions.

5.2. Magnetic Secure Transmission

Magnetic secure transmission (MST) is a payment technology for mobiles, where the mobile like the smart phones emits magnetic signals and behaves as a conventional magnetic stripe on a standard payment card (MST, 2018). It was originally evolved by LoopPay and later in 2015 was acquired by Samsung (Business Insider, 2018). SamsungPay, which is a payment method provided by Samsung, uses MST to carry out transaction. The information in MST is transmitted by the magnetic signals which are produced by the user device. Being fast and easy, the use of technology is increasing around the world.

The technology does not involve upgrading of any hardware, software or advanced technology. In comparison with NFC, MST is compatible with almost all the terminals that support the magnetic stripe reader. To keep the user card information secure it uses tokenization and is claimed to be as secure as NFC. With the increase in number of people moving towards the contactless payment, security analysis of the technology used is necessary.

5.2.1. Attacks Possible

Contactless payment mode is going to be widely used in the coming future and it is necessary check its security in terms of data privacy of the user. Since MST is claimed to be as safe as NFC, the researchers discovered some safety problems that could lead to some attacks on user data. The possible attacks are discussed below.

1. Eavesdropping

MST generates magnetic signals for communication but being a wireless communication, it is prone eavesdropping. Researchers have claimed that magnetic signal containing the encoded token can be collected through a low-cost receiver by about 2m. Depending on the direction, the distance may also be reduced. The author gathered the token by using Magspoof (Mendoza, 2016; Magspoof, 2018). Magspoof is a device that can emulate the magnetic stripe card and work wirelessly on the magnetic stripe card reader by producing the electromagnetic field. In (Choi, 2016), the author created their own magnetic signal collector and the distance of capture is at least 2 m. But the token can be captured up to 2.7 m according to (Choi & Lee, 2016).

Cloning the traditional magnetic stripe card was easy, however, cloning with MST is not feasible, but the user token eavesdrop could lead to security issues. The token is used by the user to perform any transaction and its eavesdrop might harm the transaction of the user. Proper measures are required to secure the token from eavesdropping.

2. Wormhole Attack

Wormhole attack is an attach when the attacker captures the packet from one location of the network and tunnels them to any other location in the network and retransmits the packet in another network to perform the operation. Mendoza (2016) and Choi and Lee (2018) shows how wormhole attack can be carried out in MST. Using proper jammer at the reader prevent the victim from using the token, and the captured token could be used by the attacker to perform the transaction on the victim behalf in some other network.

According to Mendoza (2016), the attacker could perform the wormhole attack by the help of Magspoof. The device can be used to capture token and can also act as a jammer to the terminal. The captured token can be transferred through email to be reused in some other environment. According to Choi and Lee (2018), the captured token is in the form of electronic signals which then passed through a software in a mobile to get the information of the token and carry out payment.

Wormhole attack indicates that there is no validation procedure for consistency between the position of the issuance of the one-time token and the place where payment happens. Proper validation of device is required to prevent the wormhole attack. Preventing wormhole attack requires to control the signal eavesdropping and developing authorization schemes. Schemes have been proposed to prevent the wormhole attack in MST which are discussed in the next section.

5.2.2. Schemes Proposed as Countermeasure

Some systems have been suggested to avoid wormhole attack in MST, which are discussed in Table 7.

Other than the schemes to avoid wormhole attack, certain schemes were also proposed to secure optimized test paths. Rathee et al. (2018), proposed a hybrid genetic tabu search and optimization algorithm to secure the optimized test paths which was achieved by Samsung pay application activity diagram. The implementation of the proposed scheme was done in C++ on the case study of online airline reservation system and Samsung pay.

Table 7. Schemes proposed to prevent attack on MST payment system

Author	Description	Advantages	Disadvantages
Cortier et al. (2017)	● Designed a protocol compatible with EMV static data authentication for payment, along with light use of secure element. ● The security of the tool was proved by Tamarin.	● Prevents wormhole attack. ● Secure from stolen key attack.	● Interaction with rogue terminal is possible. ● Token can be used until new token with greater value is not generated.
Ryu et al. (2017)	● A location authentication system whose main feature is to compare the WI provided by current user with the WM that was generated by the WI provided by previous user. ● The system does not require any changes to the POS software or additional hardware.	● Prevents wormhole attack ● Secure from key attack. ● Model is identity based and not key based.	● Entry of rogue terminal on the server database.
Bai et al. (2017)	● Demonstrated that an active attacker sniffs the token generated for payment and halts the ongoing transaction by different ways and performed the wormhole attack. ● Proposed a solution POSAUTH that adds the terminal unique identity to the payment token. ● POSAUTH binds the transaction to a particular terminal.	● Prevents wormhole attack. ● Use one way hashing to prevent sniffing and replacement.	● Static keys used in hashing and encoding.

6. TOOLS FOR SMARTCARD DEVELOPMENT

For developing the smartcard-based application and performing various test and verification of that application some open source tools are available. Other than for developing applications, tools are also available for testing and verifying the protocols developed. The open source tools are divided into different category and are discussed in Table 8.

Table 8. Open source tools for smart card development

Tool Name	Category	Description
Open Smart Card Development Platform (2018a; 2018b)	Development tool	● The Open Smart Card Development Platform (OpenSCDP) is a collection of tools for developing, testing, and deploying applications for smart cards and key public infrastructure. ● For most ISO 78164 smartcards, PC/SC and CT-API card readers, drivers are included. ● Also provides cryptographic support to algorithms which are commonly used by smart cards. ● OpenSCDP is the toolbox used in consulting services by CardContact. It has been used effectively in significant card projects and is used by multiple third-party companies for their products.
pyResMan (2018a; 2018b)	Management tool	● Open source smartcard management tool which is use for java cards and other smartcards. ● Can be used to send Application Protocol Data Unit (APDU) and execute APDU script. ● R502 SPY reader debug ISO14443 protocol commands and Mifare commands. ● Helps in managing smart card resources.
Eclipse Keyple (2018)	Open source API for contactless ticketing	● Provides generic libraries for developing contactless application based on Calypso standard. ● Calypso is a set of specification that helps in providing fast and secure off-line contactless transaction between terminal and portable object. ● Allows developer to implement fast and secure off-line contactless transactions using NFC phones and card. ● Also provides integration with the secure element which are involved in a secure contactless solution. ● Keyple is available in Java and C++.
OpenSC (2018a; 2018b)	Security library	● It is a set of software tool and library that works with smart cards and provides cryptographic capability. ● Provides the use of smart cards in security domain like digital signature, authentication and encryption.
Secunet Global Tester (2018a; 2018b)	Testing Tool	● Used for testing of smartcards, reader, and associated protocol and offers test suite based on current specification in use. ● Have capability to interpret smartcard requirements and specifications for testing.
Tamarin Prover (2018a; 2018b)	Verification Tool	● It is a verification tool for security protocol. ● Supports falsification and unbounded verification in symbolic model. ● Software protocol is specified as multiset rewriting system and are analysed with respect to first order properties and message theory.

7. WORLD-WIDE PRACTICAL APPLICATIONS

There are number of the contactless based payment applications which are in use by people world-wide. These systems eliminate the need of user to carry the cards regularly with them for payments. Carrying the cards regularly increases its risk of theft which makes the user to depend less on the cards. Some of the practical applications are discussed below.

7.1. Apple Pay

Apple Pay is a mobile payment and digital wallet service by Apple in 2014 that allows the user to make payment through smart phone. It works on the card emulation technique of NFC and supported by iPhone, iPad, Apple Watch and Mac. It is available in the United Kingdom, Canada, Australia, Croatia, Brazil, the United Arab Emirates, Saudi Arabia, Russia, Kazakhstan, China, New Zealand, Singapore, Japan, Taiwan, Hong Kong, Macau, Georgia and all countries in the European Economic Area (EEA). The main drawback is that an attacker can add a stolen card to the application.

7.2. Samsung Pay

Samsung Pay is a mobile payment and a digital wallet service provided by Samsung in 2015, in South Korea. It also works on the card emulation technique, but other than NFC it also makes use of MST for the transaction, which make it more acceptable to users than the Apple Pay which only works on NFC. Samsung Pay has grown significantly globally and is now accessible on six continents – Africa, Asia, South America, North America, Europe and Oceania. Samsung Pay is accessible in 24 countries, including the United Kingdom, Vietnam, Mexico, Italy, Canada, South Africa, Brazil, Puerto Rico, Russia, Thailand, Malaysia, South Korea, the United States, China, Spain, Singapore, Australia, India, Sweden, UAE and Switzerland. Preliminary access is also accessible in France now.

7.3. Google Pay

Google Pay is a service provided by Google to boost the in-app and tap to pay payments on mobile devices that are working on android platform. It is a new version of Google's Tez in compliance with Android Pay that was released by Google in 2018. Google Pay is available in 28 countries including – U.S, U.K, UAE, Ukraine, Taiwan, Sweden, Spain, Slovakia, Singapore, Russia, Poland, Norway, New Zealand, Japan, Italy, Ireland, Hong Kong, Germany, France, Finland, Denmark, Czech Republic, Croatia, Chile, Canada, Brazil, Belgium, and Australia.

7.4. Pockets

Pockets is an application that was proposed by ICICI bank, that works on tap & pay (Pockets, 2018). It allows the user to add ICICI bank cards to the application and perform the cashless transaction. It also works on the card emulation technique of NFC. The user can add money to the wallet using any bank's card and currently this service is available in India.

8. FUTURE RESEARCH ISSUES

8.1 Hybrid card emulation

Card emulation is a new and trending way to use the smart cards. It is mainly implemented in the payment field but if tried can be used in other smart cards applications. Models and systems could be designed whereby using the single system we can operate many applications. Hybrid smart cards exist and the same can be applied in the card emulation form with proper security measures, where a single application can hold different smart cards for different applications. Also, system can be proposed for using hybrid smartcards in card emulation form. It may give rise to technical challenges like the security parameters should be followed.

8.2. Access Control and Authentication Issues

The contactless smart cards face the access control issue because of it skimming attacks are possible. Methods are required to protect the user access to the card. In card emulation, with one pin the user gets access to all the cards which need improvement. Many schemes proposed and lacks in providing complete mutual authentication and other necessary properties. Improvement in those schemes can lead to a better method along with necessary security measures.

8.3. Malware Attacks

With the increasing malware attacks to the smart phones and various malicious applications, it is required to focus more on the security of the mobile contactless payment system and checking its security. New versions of malware like virus, Trojans, spyware, etc, are used to perform a targeted attack against the smartcards and that gives them the capability to get full control on the application based on smart cards. By stealing the login credentials attacker can get access to user private information. With the increase in the smart card application occurrences of such attack will also increase and it is therefore required to focus on the security of smart cards and mobile contactless system.

9. FUTURE SCOPE AND CONCLUSION

Over the previous few years, digital payment methods have had an incredible acceptance rate in consumer systems around the globe. Many large companies add support to all types of devices for NFC (Near Field Communication) and MST (Magnetic Secure Transmission) to enable consumers to make money transactions. Some companies use tokenization to safeguard the payment technology. These methods can be bypassed through easy mechanism. With all these changes in the payment system and the growing use in the future, the field of information security is not well prepared to protect against growing new attacks in this area. This paper has discussed the contactless smartcards and payment system in detail. The aim of the paper was to highlight the security issues in the technology used for contactless payment system along with countermeasures proposed so far. The countermeasures lack data security at various levels, which requires improvement. The paper has also included suggestions to improve the security of the contactless payment system. The article concluded with focusing on some future research issues.

REFERENCES

Rankl, W., & Effing, W. (2004). Smart card handbook. John Wiley & Sons. Report Buyer. https://www.reportbuyer.com/product/5445386

Schneier, B., & Shostack, A. (1999, May). Breaking up is hard to do: modeling security threats for smart cards. In USENIX Workshop on Smart Card Technology, Chicago, Illinois, USA, http://www. counterpane. com/smart-card-threats. html

Taherdoost, H., Sahibuddin, S., & Jalaliyoon, N. (2011). Smart card security; Technology and adoption. *International Journal of Security*, *5*(2), 74–84.

Markantonakis, K., Mayes, K., Sauveron, D., & Askoxylakis, I. G. (2008, October). Overview of security threats for smart cards in the public transport industry. In *Proceedings of the IEEE International Conference on e-Business Engineering ICEBE'08* (pp. 506-513). IEEE. doi:10.1109/ICEBE.2008.91

Aubert, B. A., & Hamel, G. (2001). Adoption of smart cards in the medical sector: The Canadian experience. *Social Science & Medicine*, *53*(7), 879–894. doi:10.1016/S0277-9536(00)00388-9 PMID:11522135

Hsu, M. H., Yen, J. C., Chiu, W. T., Tsai, S. L., Liu, C. T., & Li, Y. C. (2011). Using health smart cards to check drug allergy history: The perspective from Taiwan's experiences. *Journal of Medical Systems*, *35*(4), 555–558. doi:10.1007/s10916-009-9391-5 PMID:20703535

Chen, S. (2016). *Trust Management for a Smart Card Based Private eID Manager* [Master's thesis]. NTNU.

Conlon, J., & Whitacre, J. (2005). U.S. Patent Application No. 11/047,593.

Vanderhoof, R. (2017). *Smart Card Talk*. Alliance, SC.

Gupta, B. B., & Quamara, M. (2018). An identity based access control and mutual authentication framework for distributed cloud computing services in IoT environment using smart cards. *Procedia Computer Science*, *132*, 189–197. doi:10.1016/j.procs.2018.05.185

Gupta, B. B., & Quamara, M. (2018, October). A Dynamic Security Policies Generation Model for Access Control in Smart Card Based Applications. In Proceedings of the *International Symposium on Cyberspace Safety and Security* (pp. 132-143). Springer. doi:10.1007/978-3-030-01689-0_11

Smart Card Basics. (n.d.). Smart card overview. Retrieved from http://www.smartcardbasics.com/smart-card-overview.html

Parmar, D. N., & Mehta, B. B. (2014). Face recognition methods & applications.

Nedjah, N., Wyant, R. S., Mourelle, L. M., & Gupta, B. B. (2017). Efficient yet robust biometric iris matching on smart cards for data high security and privacy. *Future Generation Computer Systems*, *76*, 18–32. doi:10.1016/j.future.2017.05.008

Nedjah, N., Wyant, R. S., Mourelle, L. M., & Gupta, B. B. (2017). Efficient fingerprint matching on smart cards for high security and privacy in smart systems. *Information Sciences*.

Moore, S., Anderson, R., Cunningham, P., Mullins, R., & Taylor, G. (2002, April). Improving smart card security using self-timed circuits. In *Proceedings of the Eighth International Symposium on Asynchronous Circuits and Systems* (pp. 211-218). IEEE doi:10.1109/ASYNC.2002.1000311

Messerges, T. S., Dabbish, E. A., & Sloan, R. H. (2002). Examining smart-card security under the threat of power analysis attacks. *IEEE Transactions on Computers*, *51*(5), 541–552. doi:10.1109/TC.2002.1004593

Gupta, B. B., & Quamara, M. (2018). A taxonomy of various attacks on smart card–based applications and countermeasures. *Concurrency and Computation: Practice and Experience*, e4993.

Bond, M., Choudary, O., Murdoch, S. J., Skorobogatov, S., & Anderson, R. (2014, May). Chip and Skim: cloning EMV cards with the pre-play attack. In *Proceedings of the 2014 IEEE Symposium on Security and Privacy (SP)* (pp. 49-64). IEEE. doi:10.1109/SP.2014.11

Kasper, T., Oswald, D., & Paar, C. (2009, August). EM side-channel attacks on commercial contactless smartcards using low-cost equipment. In *Proceedings of the International Workshop on Information Security Applications* (pp. 79-93). Springer. doi:10.1007/978-3-642-10838-9_7

Roland, M., & Langer, J. (2013, August). Cloning Credit Cards: A Combined Pre-play and Downgrade Attack on EMV Contactless. In Presented as part of the 7th {USENIX} Workshop on Offensive Technologies. Academic Press.

Shelfer, K. M., & Procaccino, J. D. (2002). Smart card evolution. *Communications of the ACM*, *45*(7), 83–88. doi:10.1145/514236.514239

Burge, M. E. (2015). Apple Pay, Bitcoin, and Consumers: The ABCs of Future Public Payments Law. *The Hastings Law Journal*, *67*, 1493.

EMVCo. (2018). Global circulation figures. Retrieved from https://www.emvco.com/wp-content/uploads/2018/04/Global-CirculationFigures_FINAL.pdf

EMVCo. (n.d.). Deployment statistics. Retrieved from https://www.emvco.com/about/deployment-statistics/

Roberston, D. (2018, October.). *The Nilson Report*, (1140). Retrieved from https://nilsonreport.com/upload/issues/1140_0321.pdf

Eurosmart. (n.d.). Facts and Figures. Retrieved from http://www.eurosmart.com/facts-figures.html

UK Finance. (2018). UK Finance 2017 Annual Fraud update. Retrieved from https://www.ukfinance.org.uk/wp-content/uploads/2018/03/UKFinance_2017-annual-fraud-update-FINAL.pdf

Blunden, M. (2019). Surge in contactless card fraud - stealing £1.18m in 10 months. Evening Standard. Retrieved from https://www.standard.co.uk/news/crime/surge-in-contactless-card-fraud-stealing-118m-in-10-months-a4030256.html

Asokan, A. (2019). Visa Contactless Cards Vulnerable to Fraudsters: Report. Bank Info Security. Retrieved from https://www.bankinfosecurity.com/visa-contactless-cards-vulnerable-to-fraudsters-report-a-12867

Lorsch, R. H. (1999). U.S. Patent No. 5,903,633.

Barry, J. J., Newhouser, R., Rahbee, A., & Sayeda, S. (2002). Origin and destination estimation in New York City with automated fare system data. *Transportation Research Record: Journal of the Transportation Research Board*, *1817*(1), 183–187.

Infosino, W. J. (2004). U.S. Patent No. 6,715,679.

Yang, B., & Ching, A. T. (2013). Dynamics of consumer adoption of financial innovation: The case of ATM cards. *Management Science*, *60*(4), 903–922. doi:10.1287/mnsc.2013.1792

Masters, G., & Turner, P. (2007). Forensic data recovery and examination of magnetic swipe card cloning devices. *Digital Investigation*, *4*, 16-22.

Halope, C., & Zupanek, F. (2004). U.S. Patent No. 6,770,509.

Paret, D. (2005). *RFID and contactless smart card applications* (R. Riesco, trans.). Chichester, UK: John Wiley & Sons Ltd. doi:10.1002/9780470016152

Alliance, S. C. (2007). *Proximity mobile payments: Leveraging NFC and the contactless financial payments infrastructure*. Smart Card Alliance.

Lee, C. K., & Kwan, K. L. (2005). U.S. Patent No. 6,881,605.

Habraken, G. W. (2014). U.S. Patent No. 8,689,013.

Finn, D., Conneely, P. G., Czornack, J. T., Ummenhofer, K., & Lotya, M. (2015). U.S. Patent No. 9,033,250.

Kreft, H. D. (1998). U.S. Patent No. 5,773,812.

Fidalgo, J. C. (1997). U.S. Patent No. 5,598,032.

Jean, S., Donsez, D., & Lecomte, S. (2001). Using some database principles to improve cooperation in multi-application smart cards. In *Proceedings of the 21st International Conference of the Chilean Computer Science Society SCCC 2001* (pp. 154-160). IEEE. doi:10.1109/SCCC.2001.972643

Naccache, D., & M'Raihi, D. (1996). Cryptographic smart cards. *IEEE Micro*, *16*(3), 14–24. doi:10.1109/40.502402

Cuervo, V. (2001). U.S. Patent Application No. 09/894,581.

Canstar. (n.d.). What is a travel money card? Retrieved from https://www.canstar.com.au/travel-money-cards/what-is-a-travel-money-card/

Rowley, J. (2000). Loyalty kiosks: Making loyalty cards work. *British Food Journal*, *102*(5/6), 390–398. doi:10.1108/00070700010329236

Clark, P. C. (1995). U.S. Patent No. 5,448,045.

Noorhuzaimi, M. N., Junaida, S., Noraziah, A., & Chen, K. H. (2008, August). E-Visitor Information Management System (E-VIMS) using MyKad. In *Proceedings of the First International Conference on the Applications of Digital Information and Web Technologies ICADIWT 2008* (pp. 44-49). IEEE.

Abrial, A., Bouvier, J., Renaudin, M., Senn, P., & Vivet, P. (2001). A new contactless smart card IC using an on-chip antenna and an asynchronous microcontroller. *IEEE Journal of Solid-State Circuits*, *36*(7), 1101–1107. doi:10.1109/4.933467

Andersson, D. (2016). A survey on contactless payment methods for smartphones.

Lacmanović, I., Radulović, B., & Lacmanović, D. (2010, May). Contactless payment systems based on RFID technology. In *Proceedings of the 2010 Proceedings of the 33rd International Convention* (pp. 1114-1119). IEEE.

Nath, B., Reynolds, F., & Want, R. (2006). RFID technology and applications. *IEEE Pervasive Computing*, *5*(1), 22–24. doi:10.1109/MPRV.2006.13

Juels, A. (2006). RFID security and privacy: A research survey. *IEEE Journal on Selected Areas in Communications*, *24*(2), 381–394. doi:10.1109/JSAC.2005.861395

Pampattiwar, S. (2012). Literature survey on NFC, applications and controller. *International Journal of Scientific & Engineering Research*, *3*(2).

Coskun, V., Ozdenizci, B., & Ok, K. (2013). A survey on near field communication (NFC) technology. *Wireless Personal Communications*, *71*(3), 2259–2294. doi:10.1007/s11277-012-0935-5

Coskun, V., Ozdenizci, B., & Ok, K. (2015). The survey on near field communication. *Sensors (Basel)*, *15*(6), 13348–13405. doi:10.3390/s150613348 PMID:26057043

Wang, Y., Hahn, C., & Sutrave, K. (2016, February). Mobile payment security, threats, and challenges. In *Proceedings of the 2016 Second International Conference on Mobile and Secure Services (MobiSecServ)* (pp. 1-5). IEEE. doi:10.1109/MOBISECSERV.2016.7440226

Ornce, M. R., Moyer, R., Sackenheim, G. J., Dollarhide, A. B., Glenn, K. R., & Pile, S. H. (2012). U.S. Patent Application No. 13/315,544.

Samsung. (n.d.). SamsungPay tokenization. Retrieved from https://developer.samsung.com/tech-insights/pay/tokenization

Gaspar, D. (2015). U.S. Patent No. 9,092,777.

Brown, K. D., & Chatelain, D. (2008). U.S. Patent Application No. 11/875,860.

Royyuru, V. K. (2013). U.S. Patent Application No. 13/790,871.

Stapleton, J., & Poore, R. S. (2011). Tokenization and other methods of security for cardholder data. *Information Security Journal: A Global Perspective*, *20*(2), 91-99.

Chandramouli, R., Iorga, M., & Chokhani, S. (2014). Cryptographic key management issues and challenges in cloud services. In *Secure Cloud Computing* (pp. 1–30). New York, NY: Springer. doi:10.1007/978-1-4614-9278-8_1

Jawale, A. S., & Park, J. S. (2018). Towards trusted mobile payment services: A security analysis on Apple Pay. *International Journal of Internet of Things and Cyber-Assurance*, *1*(1), 76–90. doi:10.1504/IJITCA.2018.090169

Roland, M. (2012, June). Software card emulation in NFC-enabled mobile phones: great advantage or security nightmare. In *Proceedings of the Fourth International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use* (pp. 1-6). Academic Press.

Alattar, M., & Achemlal, M. (2014, August). Host-based card emulation: Development, security, and ecosystem impact analysis. In *Proceedings of the 2014 IEEE Intl Conf on High Performance Computing and Communications, 2014 IEEE 6th Intl Symp on Cyberspace Safety and Security, 2014 IEEE 11th Intl Conf on Embedded Software and Syst (HPCC, CSS, ICESS)* (pp. 506-509). IEEE.

Haselsteiner, E., & Breitfuß, K. (2006, July). Security in near field communication (NFC). In *Workshop on RFID security* (pp. 12-14). Academic Press.

Kortvedt, H., & Mjolsnes, S. (2009, November). Eavesdropping near field communication. In *Proceedings of the Norwegian Information Security Conference (NISK)* (Vol. 27, p. 5768).

Hancke, G. P. (2005). A practical relay attack on ISO 14443 proximity cards. Technical report. *University of Cambridge Computer Laboratory*, *59*, 382–385.

Francis, L., Hancke, G., Mayes, K., & Markantonakis, K. (2010, June). Practical NFC peer-to-peer relay attack using mobile phones. In *Proceedings of the International Workshop on Radio Frequency Identification: Security and Privacy Issues* (pp. 35-49). Springer. doi:10.1007/978-3-642-16822-2_4

Chothia, T., Garcia, F. D., De Ruiter, J., Van Den Breekel, J., & Thompson, M. (2015, January). Relay cost bounding for contactless EMV payments. In *Proceedings of the International Conference on Financial Cryptography and Data Security* (pp. 189-206). Springer. doi:10.1007/978-3-662-47854-7_11

Francis, L., Hancke, G., & Mayes, K. (2013). A practical generic relay attack on contactless transactions by using NFC mobile phones. *International Journal of RFID Security and Cryptography*, *2*(1–4), 92–106. doi:10.20533/ijrfidsc.2046.3715.2013.0012

Heydt-Benjamin, T. S., Bailey, D. V., Fu, K., Juels, A., & O'hare, T. (2007, February). Vulnerabilities in first-generation RFID-enabled credit cards. In *Proceedings of the International Conference on Financial Cryptography and Data Security* (pp. 2-14). Springer. doi:10.1007/978-3-540-77366-5_2

Bond, M., Choudary, O., Murdoch, S. J., Skorobogatov, S., & Anderson, R. (2014, May). Chip and Skim: cloning EMV cards with the pre-play attack. In *Proceedings of the 2014 IEEE Symposium on Security and Privacy* (pp. 49-64). IEEE. doi:10.1109/SP.2014.11

Haselsteiner, E., & Breitfuß, K. (2006, July). Security in near field communication (NFC). In *Workshop on RFID security* (pp. 12-14). Academic Press.

Fahrianto, F., Lubis, M. F., & Fiade, A. (2016, April). Denial-of-service attack possibilities on NFC technology. In *Proceedings of the International Conference on Cyber and IT Service Management* (pp. 1-5). IEEE. doi:10.1109/CITSM.2016.7577582

Chen, W., Hancke, G. P., Mayes, K. E., Lien, Y., & Chiu, J. H. (2010, April). NFC mobile transactions and authentication based on GSM network. In *Proceedings of the 2010 Second International Workshop on Near Field Communication (NFC)* (pp. 83-89). IEEE.

Chen, W. D., Hancke, G. P., Mayes, K. E., Lien, Y., & Chiu, J. H. (2010, December). Using 3G network components to enable NFC mobile transactions and authentication. In *Proceedings of the 2010 IEEE International Conference on Progress in Informatics and Computing (PIC)* (Vol. 1, pp. 441-448). IEEE.

Lee, Y., Kim, E., & Jung, M. (2013, January). A NFC based authentication method for defense of the man in the middle attack. In *Proceedings of 3rd International Conference on Computer Science and Information Technology* (pp. 10-14). Academic Press.

Ceipidor, U. B., Medaglia, C. M., Sposato, S., & Moroni, A. (2012). A protocol for mutual authentication between NFC phones and POS terminals for secure payment transactions. In *Proceedings of the Information Security and Cryptology (ISCISC)* (pp. 115-120). doi:10.1109/ISCISC.2012.6408203

León-Coca, J. M., Reina, D. G., Toral, S. L., Barrero, F., & Bessisb, N. (2013). Authentication Systems Using ID Cards over NFC Links: The Spanish Experience Using DNIe. In Proceedigns of the 4th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN-2013) (Vol. 21, pp. 91–98). Academic Press. doi:10.1016/j.procs.2013.09.014

Thammarat, C., Chokngamwong, R., Techapanupreeda, C., & Kungpisdan, S. (2015, January). A secure lightweight protocol for NFC communications with mutual authentication based on limited-use of session keys. In *Proceedings of the 2015 International Conference on Information Networking (ICOIN)* (pp. 133-138). IEEE. doi:10.1109/ICOIN.2015.7057870

Nashwan, S. (2017). Secure Authentication Protocol for NFC Mobile Payment Systems. *International Journal of Computer Science and Network Security*, *17*(8), 256–262.

MST. (n.d.). Samsung. Retrieved from https://www.samsung.com/global/galaxy/what-is/mst/

Villas-Boas, A. (2015, September 24). Samsung has a key technological advantage that makes it much better to pay with your phone. *Business Insider*. Retrieved from https://www.businessinsider.in/Samsung-has-a-key-technological-advantage-that-makes-it-much-better-to-pay-with-your-phone/articleshow/49083595.cms

Mendoza, S. (2016, July). Samsung pay: Tokenized numbers, flaws and issues. In Proc. Black Hat USA (pp. 1-11). Academic Press.

Magspoof. (n.d.). Retrieved from https://samy.pl/magspoof/

Choi, D., & Lee, Y. (2016). Eavesdropping one-time tokens over magnetic secure transmission in Samsung Pay. In *Proceedings of the 10th USENIX Workshop on Offensive Technologies (WOOT 16)*. Academic Press.

Choi, D., & Lee, Y. (2018). Eavesdropping of Magnetic Secure Transmission Signals and Its Security Implications for a Mobile Payment Protocol. *IEEE Access: Practical Innovations, Open Solutions*, *6*, 42687–42701. doi:10.1109/ACCESS.2018.2859447

Cortier, V., Filipiak, A., Florent, J., Gharout, S., & Traoré, J. (2017, April). Designing and proving an EMV-compliant payment protocol for mobile devices. In *Proceedings of the 2017 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 467-480). IEEE.

Ryu, G., Seo, C., & Choi, D. (2017). Location authentication based on wireless access point information to prevent wormhole attack in Samsung Pay. *Advances in Electrical and Computer Engineering*, *17*(3), 71–77. doi:10.4316/AECE.2017.03009

Bai, X., Zhou, Z., Wang, X., Li, Z., Mi, X., Zhang, N., . . . Zhang, K. (2017, August). Picking Up My Tab: Understanding and Mitigating Synchronized Token Lifting and Spending in Mobile Payment. In *Proceedings of the 26th USENIX Security Symposium (USENIX Security 17)* (pp. 593-608). USENIX Association.

Rathee, N., & Chhillar, R. S. (2018). Model driven approach to secure optimized test paths for smart Samsung Pay using hybrid genetic tabu search algorithm. *International Journal of Information System Modeling and Design*, *9*(1), 77–91. doi:10.4018/IJISMD.2018010104

Open Smart Card Development Platform. (n.d.). Retrieved from https://www.openscdp.org/

Open Smart Card Development Platform. (n.d.). Retrieved from https://www.openscdp.org/screenshot.html

pyResMan. (n.d.). Retrieved from https://www.javacardos.com/tools/pyresman

pyResMan. (n.d.). Retrieved from https://sourceforge.net/projects/pyresman/

ECLIPSE. (n.d.). Retrieved from https://www.eclipse.org/community/eclipse_newsletter/2018/october/keyple.php

OpenSC. (n.d.). Retrieved from https://github.com/OpenSC/OpenSC/wiki

Wikipedia. (n.d.). OpenSC. Retrieved from https://en.wikipedia.org/wiki/OpenSC

Secunet Global Tester. (n.d.). Retrieved from https://www.secunet.com/en/products-solutions/globaltester/

Secunet Global Tester. (n.d.). Retrieved from https://globaltester.secunet.com/fileadmin/user_upload/secunet_FS_GlobalTester_GB.pdf

Tamarin Prover. (n.d.). Retrieved from https://tamarin-prover.github.io/manual/book/001_introduction.html

Pockets. (n.d.). ICICI Bank. Retrieved from https://www.icicibank.com/Personal-Banking/bank-wallet/pockets/pockets.html

Gupta, B. B. (Ed.). (2018). *Computer and cyber security: principles, algorithm, applications, and perspectives*. CRC Press.

Almomani, A., Gupta, B. B., Wan, T. C., Altaher, A., & Manickam, S. (2013). Phishing dynamic evolving neural fuzzy framework for online detection zero-day phishing email.

Jiang, F., Fu, Y., Gupta, B. B., Lou, F., Rho, S., Meng, F., & Tian, Z. (2018). Deep learning based multi-channel intelligent attack detection for data security. *IEEE transactions on Sustainable Computing*.

Li, D., Deng, L., Bhooshan Gupta, B., Wang, H., & Choi, C. (2019). A novel CNN based security guaranteed image watermarking generation scenario for smart city applications. *Information Sciences*, *479*, 432–447. doi:10.1016/j.ins.2018.02.060

Li, J., Yu, C., Gupta, B. B., & Ren, X. (2018). Color image watermarking scheme based on quaternion Hadamard transform and Schur decomposition. *Multimedia Tools and Applications*, *77*(4), 4545–4561. doi:10.1007/s11042-017-4452-0

B. B. Gupta received his PhD degree from Indian Institute of Technology Roorkee, India in the area of information security. He has published more than 200 research papers in international journals and conferences of high repute. He has visited several countries to present his research work. His biography has published in the Marquis Who's Who in the World, 2012. At present, he is working as an Assistant Professor in the Department of Computer Engineering, National Institute of Technology Kurukshetra, India. His research interest includes information security, cyber security, cloud computing, web security, intrusion detection, computer networks and phishing.

Shaifali Narayan completed her Master's degree in Cyber Security from National Institute of Technology, Kurukshetra, India. She received her Bachelor's degree in Computer Science and Engineering from Invertis University, Bareilly, India, in 2015. Her research interest includes cyber security, web security, information security, smartcards, payment system security and Internet of Things (IoT).