International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Secure Transaction by MIFARE Cards using NFC Technology

Tejaswini P Chinde[1], Deepika Dash[2]

[1]M.Tech CNE, Department of CSE, R.V College of Engineering, Bengaluru, Karnataka, 560040, India

[2]Assistant Professor, Department of CSE, R.V College of Engineering, Bengaluru, Karnataka, 560040, India

Abstract: ***With improvement in mobile technology, the usage of mobiles in day to day lives of people has increased and handling of it is a difficult task. The ideal solution evolved for secure transaction is MIFARE cards. MIFARE cards are the smart cards which have security mechanism embedded in the secure element or the chip to provide secure transactions and it operates with NFC (Near Field Communication) technology where communication happens between two NFC enabled devices within the range of 10cm. MIFARE cards have different applications like public transport, parking, movies and concert tickets, E- payments, E- passport etc.***

Keywords: AES - Advance Encryption Standard, APDU - Application Protocol Data Unit, CAPDU - Command APDU, DES - Data Encryption Standard, ISO/IEC - International Organization for Standardization/ International Electro technical Commission, JCOP - Java Card Operating Platform, NFC - Near Field Communication, OTA - Over The Air, RAPDU - Response APDU, RFID - Radio Frequency Identification, VCM - Virtual Card Management.

1. Introduction

As advancement in technology especially in wireless communication is trending but it has its own security breaches. Now a day there is more usage of mobile devices in daily lives of people leads to an intension to easier the works of people by using MIFARE card for secure transactions. MIFARE cards are NXP Semiconductor's proprietary for Smart cards which are a computing chip that has memory and microprocessor for storing and processing the data [1]. The MIFARE cards uses NFC (Near Field Communication) technology i.e. the communication between two NFC enabled devices which happens in the range of 10 cm, 13.56 MHZ and is an advance technology to RFID [1]. Each MIFARE cards has operating system depending upon application, the common used OS are JCOP (Java Card Open Platform), MultiOS, windows for smart card, etc. For any online transactions there are many security challenges and breaches or issues to be considered [2]. Each MIFARE cards implement different algorithms such as AES, DES, 3DES, Crypto1 etc. for providing security for those applications. It under goes MIFARE for mobile methodology where the service provider has a right to access the secure element from remote and manage it from a single interface over the air (OTA).

2. MIFARE card and its variants

MIFARE cards perform secure transactions using MIFARE for Mobile methodology using NFC technology where MIFARE for Mobile is over the air (OTA) process that is the single interface which is available for service provider to access remotely to the secure element and manage it. There are variants of MIFARE cards like Classic, DESFire, Ultralight and Plus [3]. These variants have its own feature and algorithm implemented depending upon the desired application requirement and is explained as below and is as shown in below figure 1 different MIFARE cards.

Figure 1: MIFARE cards

MIFARE Classic: In MIFARE cards classic was the first card developed which is later lead to evolution of other cards. It has two types based on memory configuration size that is 1K and 4K bytes. It performs Crypto1 algorithm and follows ISO/IEC 14443 -3. It is used for single application usage like Employee or student or campus cards, car parking, public transportation etc. [3]

MIFARE DESFire: It is improvised card in terms of security and application based. It stands for DES algorithm used in it and FIRE refers "Fast, Innovation, Reliable and sEcure". The algorithms that can be implemented in it are DES, 3DES, AES. Its memory configuration types are 2K, 4K and 8K bytes. It also supports ISO/IEC 14443 – 3 and 4 standards [3].

MIFARE Ultralight: It is the light weighted physical cards as its name depicts. It is used in limited use application like movie, concert tickets etc. No security is provided by these cards and there is no implementation of any algorithm depending upon applications and it supports ISO/IEC 14443 – 3, but in Ultralight C card it implements 3DES algorithm [3].

MIFARE Plus: It has multiple security levels like level 0, 1 and 2 depending on application requirements and it has backward compatibility feature implemented. It can follow Crypto1 and AES algorithms [4]. It has Memory of 2K, 4K bytes and adopted for all ISO/IEC 14443 standards that is from 1 – 4. It is compatible with MIFARE Classic card [3].

These different cards of MIFARE can be implemented in single secure element of NFC enabled mobiles where individual card can be accessed according to required application at a time. The access is done through Virtual card management (VCM) process. Due to these algorithms implemented in MIFARE cards, it provides high security while any application [5].

3. System Architecture and Flow chart

The over view of MIFARE transaction system architecture is as shown in below figure 2 where the communication happens over the air interface that is through contactless. The methodology implemented in MIFARE cards is MIFARE for mobile which is the process where transactions or communication is through contactless interface over the air between card and the reader and the both devices should be NFC enabled. First card or end user is identified from the back end database if it is authenticated device or user it's allowed for further communication with the reader or the terminal. The communication occurs in APDU (Application Protocol Data Unit) format that is as per ISO standards. The commands sent from terminal or reader to card is CAPDU (Command Application Protocol Data Unit) and the response from card to reader is RAPDU (Response Application Protocol Data Unit).

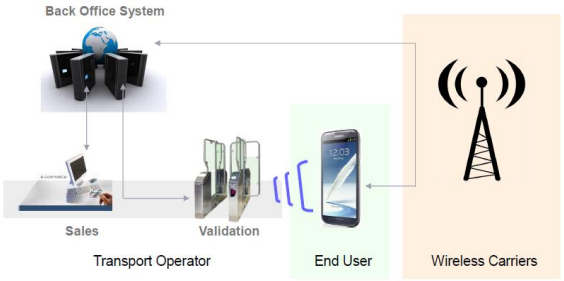

Figure 2: MIFARE Transaction system architecture

The flow of MIFARE transaction is as shown in below Figure 3. It can be seen that the NFC technology works within the range of 10cm and makes the card to be in ready or ON state for establishing the session with terminal or reader. As explained above it identifies the end user or card from database if validates correctly it proceeds further steps. Later it initializes the particular card and checks for any anti – collision status if status is clear it validates its identity and activates the authenticated card [6]. After activating it is now available for communication or any transactions in APDU format packet.

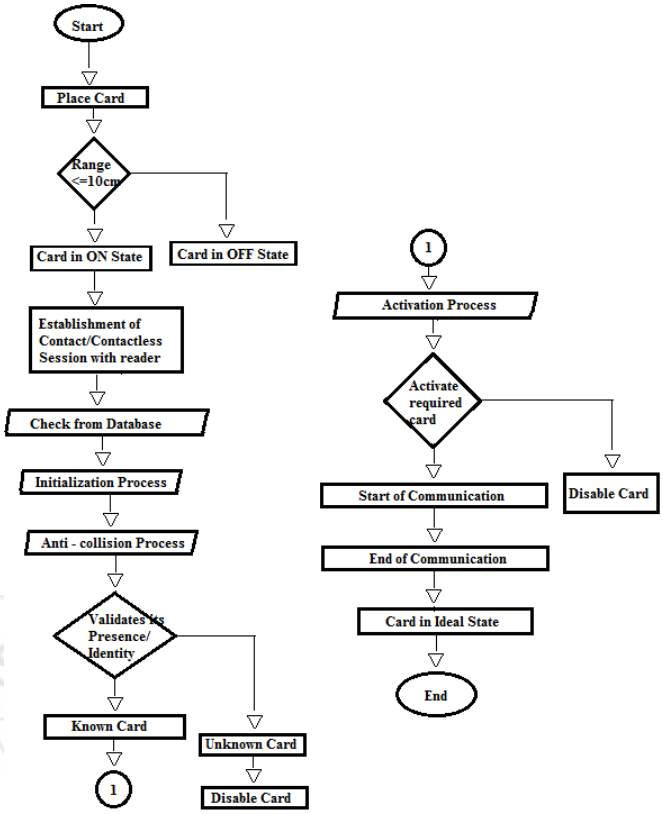

Figure 3: Flow diagram of MIFARE Transaction

Next section explains the data flow diagram of automated test of the system.

4. Data Flow Diagram of Automation Test

The data flow diagram of automation test of MIFARE transaction system is as shown in below figure 4. For every automation test it first updates the project by checking out the right path from repository and set the environment such as JAVA home to prepare for the build of test bench. Schedule the tasks to be performed and run the test cases and check there respective logs, if found any errors change the scripts accordingly, update and run again until fixes are made. Each run generates the report for implementation, analysis and for future use as a record.

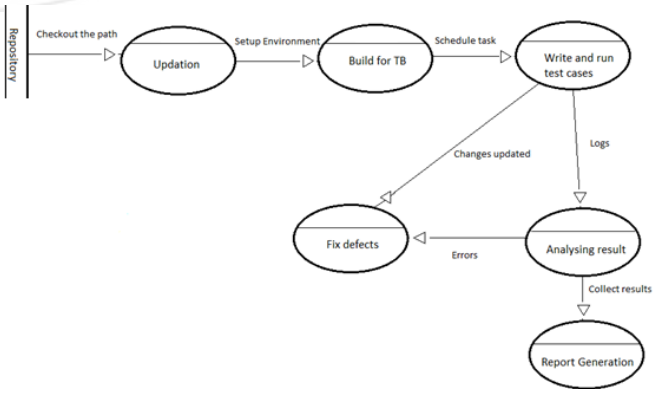

Figure 4: Data flow diagram of Automation level of MIFARE Transaction

Next section shows the experiment conducted for MIFARE cards transaction with the test results.

5. Test Results

Tests for different JCOP (Java Card Open Platform) versions has been conducted to check the total time required in execution by the MIFARE cards in general and is as shown in below figure 5. It depicts the version 1 requires 0.06974 sec, version 2 needs 0.060413 sec, and the latest JCOP version that is version 3 takes around 0.057222 sec. It is observed that on an average the time taken is around 0.057222 sec for various run of JCOP version 3 latest (Run1: 57222, Run2: 57275, Run3: 57122 microseconds).

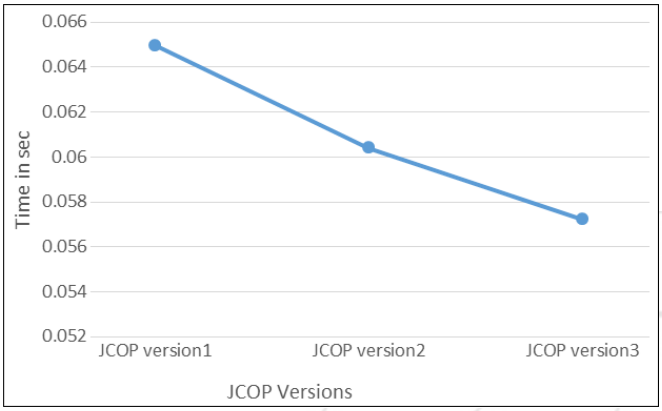

Figure 5: Comparison of different JCOP version for total execution time by MIFARE cards

Above details provided the experiment conducted for different JCOP version. In next section we would conclude the experiment conducted.

6. Conclusion

In this paper we explained the MIFARE cards and its variants available, the features implemented in each cards. Depending upon the security requirements required in application the respective MIFARE cards is been selected. It is observed that MIFARE cards provide high security in online transactions or payments. The application where lowest security is needed there MIFARE Ultralight cards are been used and if high security application we can opt for MIFARE DESFire cards. Reducing carrying different cards for different application single secure element with these cards implemented in mobiles is used by virtual card management. For experimental analysis MIFARE cards provide high speed, easy and secure transactions or payment.

7. Acknowledgment

We would like to thank the Company NXP Semiconductors, Manager Guru Prasad, Mentor Mohan Ram, team members for their help and support in improving, understanding the experiment conducted. Also, we like to thank R. V. College of Engineering, Dept. of CSE, guides and lectures for their moral support and timely guidance.

References

[1] Wolfgang Rankl and Wolfgang effing, “Smart card Handbook”, manual third edition, NXP Semiconductors, 2003
[2] Niranjanamurthy M, DR. DharmendraChahar, “The study of E-Commerce Security Issues and Solutions”, *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 2, Issue 7, July 2013, pp. 1-12
[3] NXP Semiconductors,“NXP Reader Library Peer to Peer user Manual”, Rev.24 July 2013.
[4] Joan Daernen, Vincent Rijrnen, “The Design of Rijndael,AES - The Advanced Encryption Standard”, Springer-Verlag Berlin Heidelberg New York, 2002, ISBN 3-540-42580-2
[5] M. Renaudin, F. Bouesse, Ph. Proust, J. P. Tual, L. Sourgen, F. Germain, “High security smartcards”, *Proceedings Design, Automation and Test in Europe Conference and Exhibition*, Vol. 1, 2004, pp 228 - 232
[6] S. Nivetha, N. Edna Elizabeth, T. PrasanyaPadmasha, I. Gohulalakshmi, “Secure authentication process in smart cards”, *10th International Conference on Intelligent Systems and Control (ISCO)*, 2016, pp. 1-6