International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 06 | Jun 2022 www.irjet.net p-ISSN: 2395-0072

Accessory authentication on NFC enabled product using three pass AES algorithm

Sukrutha C Basappa[1], Nagaraja G S[2]

[1]*MTech student at R V College of Engineering, Bengaluru, Karnataka*
[2]*Professor and Associate Dean (PG-CSE) at R V College of Engineering, Bengaluru, Karnataka*

Abstract - *Nowadays, Near Field Communication (NFC) market is no more a monopoly. Competition is high among the companies with regard to products they manufacture and their features for consumer attraction. Mutual authentication between NFC reader and tag ensures safe communication between them. This paper proposes an accessory authentication model that guarantees that counterparts of a product are of same company. AES-128 bits algorithm is used in two different modes, that is AES-ECB and AES-CBC for mutual authentication. AES-CBC mode is stronger in terms of security when compared to AES-ECB mode.*

Key Words*: AES, Brand protection, Mutual authentication, NFC, Security.*

1. INTRODUCTION

NFC technology was developed in the year 2004 by Philips Electronics and Sony. It is a short range, wireless technology with operating area within 10 centimeters, operating frequency 13.56 MHz and data transmission rate used here is of 106 kbps. The objective of the paper is to develop an accessory authentication model for an NFC enabled product. This ensures that replaceable part of the product (NFC tag) and the fixed part (active NFC reader) are paired counterparts and are of the same company. With this end-user can get high quality product. This kind of product positively impacts manufacturing and authenticating companies, thereby ensuring brand protection. Some examples are authentication in motorized tooth brush, where brush handle has NFC reader and the brush head has NFC tag in it. In high end blenders, the base unit will have NFC reader and the jar/container will have NFC tag.[12] To achieve this, firstly communication is established among the NFC reader and the tag. Then three pass AES (Advanced Encryption Standard) algorithm is run, before actual data transfer happens. AES-128 is a symmetric block cipher, that uses one shared secret key for both encryption and decryption. Choice for mode of AES is provided. User can choose authentication to happen either in AES-ECB (Electronic Code Book) or in AES-CBC (Cipher Block Chaining) mode, depending on their requirement.

2. LITERATURE SURVEY

In [1], authors have used the fact that NFC has an operating mode called read or write. This has the property of one directional transfer of data only. However, they have tried to bring in a bi-directional model that is half duplex in nature. Main advantage of this operating mode of NFC is that, it allows different data formats and very low protocol overhead. But one main challenge is regarding the reader collision problem, completing transactions in a secure way, within a time frame. Fingerprint and Kerberos are two factor authentication used.

In [2], a smart bandage with wireless temperature and strain sensor, with passive NFC tag is designed. An android application called SenseAble was built, to display the body temperature and other sensor readings. Chest expansion and contraction of a Covid-19 patient was rightly monitored by this smart bandage.

In [3], it proves that MITM attacks can be done during NFC communication, when using a passive card. This method of attack mimics real implementation of EMV protocol enabling devices, used for payments. Paper demonstrates how a contactless payment system can be compromised by an attacker, by using a malicious MITM card.

In [4], study is done on reading range of implanted sensors, based on NFC Integrated circuit (IC) by using a NFC enabled smart phone. Challenges noted were low coupling between loops of various sizes and limited quality imposed by bandwidth communication. Results show that system with three coils performs better at longer distance than 2-coil system.

In [5], a scheme to build a new public transport payment method with different technologies like NFC, Bluetooth, IC card is integrated. Advantage is that, passengers can choose the payment method that suits them, in terms of discount on ticket fare. This solves the problem that the payment platforms are not unified and that passengers have many applications on their mobile, which causes inconvenience while travelling.

In [6], a model for vehicle network operators using NFC is proposed. Tourists generally will not use local mobile operator's services, as they stay for short time and the roaming charges are also high. As a solution, the model which allows less mobile traffic cost for tourist and has increased transaction security is proposed. Here the user's mobile traffic is routed to the network of vehicle rental service

provider. This simplifies the tourism for a tourist and security of user's personal data.

In [7], author starts the paper by discussing general aspects of NFC and its comparison with RFID technology. Light is thrown on different ISO standards NFC complies with and NFC operating modes. They prove that NFC is vulnerable to security attacks, which can leak user's important data. This can have negative impact on organization adopting NFC technology and its applications. Different attacks are listed and a scientific method to increase security is also proposed.

In [8], extended version of different attacks in NFC area is briefed. Focus on DoS and data corruptions was given as it was noted from studying risk assessment models, these two attacks were most commonly witnessed. They were studied by Analytical Hierarchy Process (AHP). A solution was proposed which was a touch and go application called MIDAS. It is concluded that AES and ECC (Elliptic Curve Cryptography) are best known algorithms to build a secure channel and to avoid data corruption.

In [9], Authors propose an application of NFC in the IoT domain. Textile industry is far behind in terms of IoT. Hence, to enhance the textile business, a system called 'Interactive clothes' is designed. Every cloth has an NFC chip with unique number embedded in it. An application to scan the NFC is developed, which gives a URL to the database. This system modernises manufacturing, managing, selling and buying goods.

In [10], author proves that tags used in NFC system are limited in terms of chip size and power consumption. These limitations make it difficult to integrate strong cryptographic security onto the tags. Author suggests that there is need to implement secure algorithm that is secure against attack like Side-Channel Analysis (SCA). As a case study, a tag with cryptographic algorithms (AES and ECDSA) implemented is taken.

Few of the research gaps observed are as follows:

1. NFC is a short-range communication technology, and hence believed that security risks are low as the interaction is within close proximity. But security vulnerabilities do exist and few attacks are only discovered.

2. NFC is mostly used in the area of access control and payment method. Other applications like file transfer and in IoT can be researched more.

3. The economic performance of NFC developments can be evaluated and impacts of NFC technologies on companies, organizations and business models can be explored.

3. DESIGN

Project design gives an outline of project development process. It helps to identify the modules and the tools required to implement them. Figure 1 shows the system architecture which includes a user application built on NFC reader library for authentication process [11]. The reader library stack has four layers. Application layer is the top layer, which implements the commands to work with contactless technologies. Protocol abstraction layer has functions for NFC card activation. The hardware specific elements of reader implemented in the hardware abstraction layer. It also helps execute native commands of the chip. The lowest bus abstraction layer, implements the communication between the reader and tag. Both reader and tag have a key store, from which they decide upon a secret key for authentication.

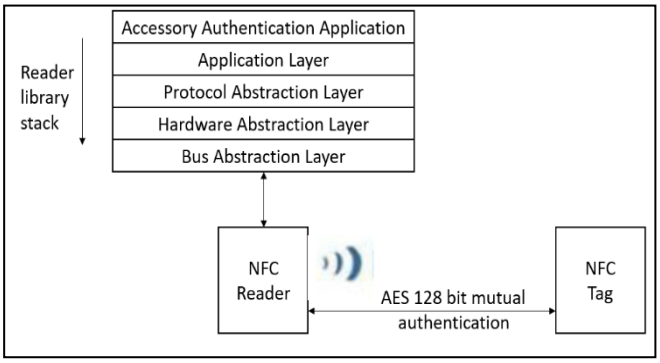

Figure 1: System architecture

Data flow diagrams help to understand the system better as it brings in modularity. Figure 2 shows DFD Level 0. Authentication procedure starts when user application makes reader to pass ReqA (Request A) command to the detected cards. Authentication result is decisive, if counterparts are authenticated then communication between them starts, else aborts.

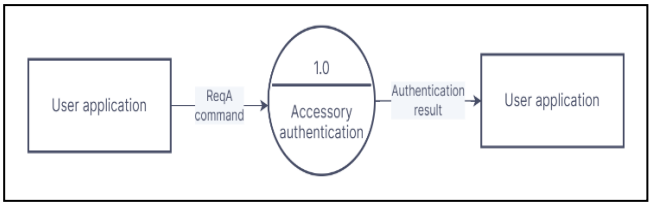

Figure 2: DFD Level 0

DFD Level 1 in figure 3 shows the two modules involved in accessory authentication. First is communication establishmemt between reader and tag, which is achieved by using available command set of tags. If more than one card is present in proximity, collision resolution is done by standard anticollision procedure and one card is selected. Then three pass AES algorithm is used for mutual authentication.

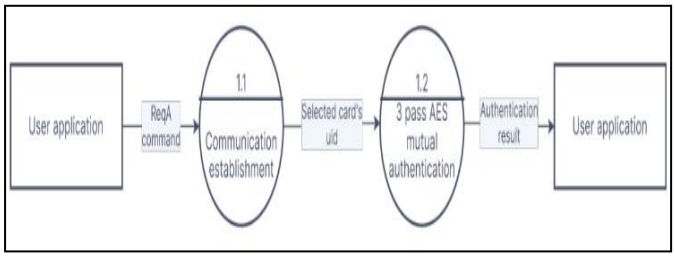

Figure 3: DFD Level 1

4. METHODOLOGY

NFC reader will emit radio waves in a periodic manner and checks if any card is present in its proximity. If no card is detected, reader continues the loop until a card is detected. If more than one card is detected, anticollision procedure resolves the conflict and chooses one card as counterpart for reader. After card selection and activation, authentication procedure happens. If reader and tag successfully authenticate to each other, a sample text is written into the card and then read back to check data integrity. Figure 4 shows entire methodology adopted in the form of flowchart.

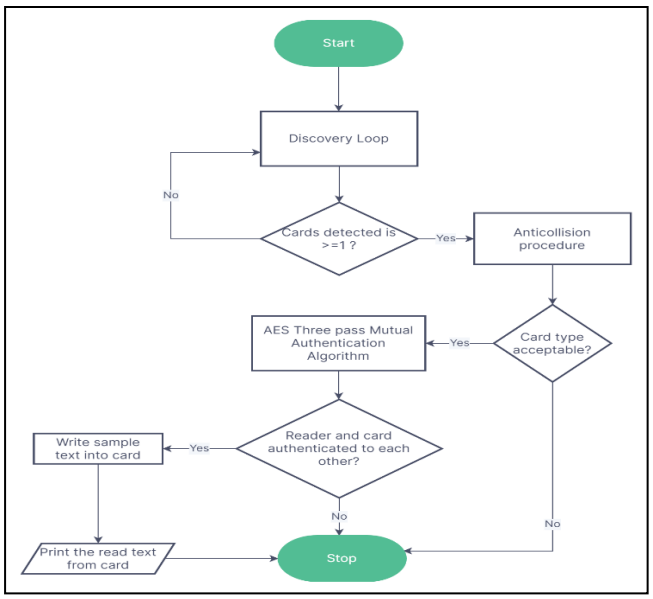

Figure 4: Flowchart of accessory authentication

AES three pass mutual authentication is a procedure which uses key of length 128 bits [12]. In the first pass of algorithm, NFC reader encrypts its data (RndX) with agreed secret key (K) and sends the cipher to NFC tag. In return, tag responds by sending the deciphered data. In second pass, tag encrypts its data (RndY) and sends the cipher generated to reader. Reader deciphers and sends the response back. Third pass includes each party verifying if data received is same as what they had generated originally. That is reader checks if tag had sent RndX correctly, and tag checks if reader's response had RndY. If any one party fails to authenticate themselves to other, the accessory authentication procedure is aborted. User can choose either AES-ECB mode for authentication or AES-CBC mode. If data being enciphered by each party is not sensitive, ECB is best option as it is fast. However, if security of data is prime concern, then CBC is preferred because of its complexity. Figure 5 shows pictorial representation of authentication procedure discussed above.

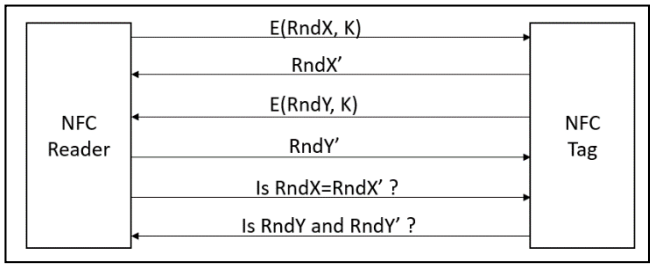

Figure 5: Three pass mutual authentication

5. RESULT AND ANALYSIS

Anticollision procedure selects a tag based on its uid (unique identification number) which is followed by card activation. The console display is as shown in figure 6. Technology of the detected card is displayed along with its uid.

```
SEGGER J-Link GDB Server V7.64e – Terminal output channel

Starting discovery loop...
Card detected and activation is done successfully
Selected card details - Technology: Type A
                        UID: 03 27 1F 81 DE 51 90
```

Figure 6: Card activation

Card activation is followed by choice entry by user for mode selection. The output after running accessory authentication in AES-CBC mode is shown in figure 7. Both reader and tag have authenticated to each other. Sample text was written into tag and read successfully without any error.

```
SEGGER J-Link GDB Server V7.64e – Terminal output channel

----------Accessory Authentication Application----------
Press 1 to begin authentication in AES-ECB mode
Press 2 to begin authentication in AES-CBC mode
Enter your choice: 2
Mutual authentication was successful. . . . .

Writing sample text into tag
. . . . . DONE
Reading data from tag
. . . . . SUCCESS
```

Figure 7: Accessory authentication by AES-CBC mode

AES-ECB mode is simple and fast approach. Drawback is that duplicate data in plain text will be reflected in the cipher text. Hence, it is not recommended in the areas where security is a priority. Whereas, AES-CBC mode will encrypt every occurrence of same plain text into different cipher text. But it is slow and complex compared to ECB mode. Yet CBC is stronger in terms of security and is preferred for authentication.

6. CONCLUSION

A survey shows that NFC market is likely to raise from 18 billion USD in 2020 to 34.9 billion USD by 2025. The main use cases are in mobile commerce and usage of wearable technology. This paper serves the need for accessory authentication by AES algorithm, to ensure that genuine parts of same company are used. This enhances consumer experience, convenience and ensures product safety. If product requires more secure form of authentication, ECC is suggested from public key cryptographic algorithms. Here, user application just checks read and write onto the tag after successful authentication. This feature can be enhanced according to user needs. Example in case of NFC enabled product like motorized toothbrush, authentication can be followed by tapping mobile phone to tag can display URL to webpage that keeps track of oral health and brush head replacement date.

REFERENCES

[1] M. S. Chishti, C. T. King and A. Banerjee, "Exploring Half-Duplex Communication of NFC Read/Write Mode for Secure Multi-Factor Authentication", 2021 in IEEE Access, vol. 9, pp. 6344-6357, doi: 10.1109/ACCESS.2020.3048711.

[2] P. Escobedo, M. Bhattacharjee, F. Nikbakhtnasrabadi and R. Dahiya, "Smart Bandage With Wireless Strain and Temperature Sensors and Batteryless NFC Tag", 2021, in IEEE Internet of Things Journal, vol. 8, no. 6, pp. 5093-5100, 15 March, doi: 10.1109/JIOT.2020.3048282.

[3] S. Akter, S. Chellappan, T. Chakraborty, T. A. Khan, A. Rahman and A. B. M. Alim Al Islam, "Man-in-the-Middle Attack on Contactless Payment over NFC Communications: Design, Implementation, Experiments and Detection", 2021, in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 6, pp. 3012-3023, 1 Nov-Dec, doi: 10.1109/TDSC.2020.3030213.

[4] A. Lazaro, M. Boada, R. Villarino and D. Girbau, "Study on the Reading of Energy-Harvested Implanted NFC Tags Using Mobile Phones", 2020 in IEEE Access, vol. 8, pp. 2200-2221, doi: 10.1109/ACCESS.2019.2962570.

[5] C. Shuran and Y. Xiaoling, "A New Public Transport Payment Method Based on NFC and QR Code", 2020 IEEE 5th International Conference on Intelligent Transportation Engineering (ICITE), pp. 240-244, doi: 10.1109/ICITE50838.2020.9231356.

[6] V. Oliinyk and O. Rubel, "Improving Safety and Ease of Use in Automatic Electric Vehicle Rental Systems", 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), pp. 800-803, doi: 10.1109/TCSET49122.2020.235545.

[7] A. Albattah, Y. Alghofaili and S. Elkhediri, "NFC Technology: Assessment Effective of Security towards Protecting NFC Devices & Services", 2020 International Conference on Computing and Information Technology (ICCIT-1441), 2020, pp. 1-5, doi: 10.1109/ICCIT-144147971.2020.9213758.

[8] M. M. Singh, K. A. A. K. Adzman and R. Hassan, "Near Field Communication (NFC) Technology Security Vulnerabilities and Countermeasures",2018, International Journal of Engineering & Technology, vol. 7, no. 4.31, pp. 298-305.

[9] Kishore Kumar Reddy N. G. and Rajeshwari K., "Interactive clothes based on IOT using NFC and Mobile Application", 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), 2017, pp. 1-4, doi: 10.1109/CCWC.2017.7868339

[10] Korak T, "Evaluation of a security-enabled NFC Tag with AES and ECDSA", 2011, Master's thesis, Institute

for applied Information Processing and Communications (IAIK), Austria.

[11] NFC Reader Library: https://community.nxp.com/pwmxy87654/attachments/pwmxy87654/nfc/707/1/UM10802_NXP-NFC-Reader-Library-v3.010-API.pdf

[12] Mutual authentication procedure: https://community.nxp.com/pwmxy87654/attachments/pwmxy87654/tech-days/179/1/AMF-SMC-T3036.pdf

BIOGRAPHIES

Sukrutha C Basappa, is a MTech student at Department of Computer Science and Engineering, R V College of Engineering, Bengaluru, Karnataka, India. (sukruthacb.scn20@rvce.edu.in)

Dr. Nagaraja G S, is working as Professor and Associate Dean (PG-CSE) at Department of Computer Science and Engineering, R V College of Engineering, Bengaluru, Karnataka, India. (nagarajags@rvce.edu.in)