International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org, editorijettcs@gmail.com
Volume XX, Issue XX, May-June 2022 ISSN 2278-6856

Comparative Study of Security Algorithms for NFC Technology

Pooja Hadli[1], Dr. Shushrutha K S[2]

[1] Department of ECE,
R V College of Engineering Bengaluru,

[2] Department of ECE
R V College of Engineering Bengaluru

Abstract: ***The main aim of this paper is to provide security algorithms for NFC technology, which enables NFC to be used in day to day life, making simpler, smarter and secure life. The security algorithms are incorporated in NFC technology for various accessories authentication, authenticated access control, ticket authentication in public transport or cinema, concerts. Thereby improves the supply chain and values insights of the consumer. Near field communication is shorter range up to 10cm wireless communication uses a base frequency of 13.56 MHz. NFC due to its shorter range provides the security to some extent . So the NFC offer digital authentication which helps to avoid duplication of tickets, consumer accessories. Nowadays many smartphones are also equipped with NFC technology, which makes smarter and secure consumables. Therefore in order to authenticate the NFC uses the security algorithms such as AES and DES, though these are the basic algorithms provides simpler computations.***

Keywords: Near Field Communication (NFC), Advanced Encryption Standard (AES), Data Encryption Standard (DES), Man in the Middle (MITM), Radio Frequency Identification (RFID), Elliptical Curve Cryptography (ECC)

1. INTRODUCTION

NFC technology mainly known to the world via mobile payments, as it plays important role in payment modes. So NFC technology being extended to health apps, various NFC supported payment apps are entering the market such as apple pay, google pay. Therefore security is one of important aspect, since the people using NFC technology for various applications and connected to the smarter world, it is important to safeguard the usability, integrity, value and continuity through secure approach. Amidst other wireless communications like RFID, Bluetooth, Wi-Fi and ZigBee, NFC outstands the other technologies, as NFC has the shortest range for transmission and also the high frequency implies smallest data rate among wireless communications and requires low power. Moreover, the significant advantage of NFC over other technologies is the shorter set-up time as it uses inductive coupling which takes less than one tenth of a second to establish a connection between two devices and it also provides a higher degree of security, which certainly makes NFC suitable for crowded areas where it correlates a signal with its transmitting physical device. NFC is typically centered on RFID, whereas Bluetooth or Wi-Fi are based on spread-spectrum technology [1]. NFC communication establishment consists of an initiator and a target. The initiator begins the communication and is typically an active NFC device which energies the target if the target device is a passive device as it possesses an energy component which can generate power for the target as well. The target device can either be an RFID tag or a RFID tag-based card. The target devices respond to the requests generated by the initiator in the form of responses. Hence the both initiator and target device are required to authenticate using AEs and DES security algorithms.

This paper proposes the AES and DES algorithms for the NFC technology. The main goal is to present AES 128 bit and DES security algorithms in various use cases of NFC for example setup services in pairing of WIFI, Bluetooth and other wireless technologies and then handover the communication after initial pairing. It is required to have authenticated pairing between the communicating devices to avoid the eavesdropping, Man in middle attack, reply attacks and data corruption. Thus security has become very important in the NFC technology. The security algorithms proposed for authentication are AES 128 bits and DES symmetric key algorithms.

2. RELATED WORK

The NFC technology is widely used in various domains such as payment application, smart phones, ticketing for transport, identity authentication and so on. Therefore researchers carried out various researches and have written research articles and papers through their work on security in NFC applications. In [1] authors have exploited the potentials of NFC technology over other wireless connectivity technologies like Wi-Fi, Bluetooth and ZigBee, these were primarily focused on read/write mode of the NFC which was intended using unidirectional data transfer between active NFC reader to passive NFC tag. Resulting in allowing various data formats and truncated protocol overhead in read/write mode of NFC. A secure multi Factor authentication system for mutually authenticating two NFC devices proposed to provide the authenticity. In [2] brief about security attacks such as Man

in the Middle (MITM) attack which are practically feasible in NFC communication (by passive card). These technique of attack performs as EVM protocol assisting devices which are used mainly for payment. Therefore this scheme for detection of attack during channel switching through incremented time delay. In [3] provides solution to low coupling between the antenna loops and shortcomings of quality caused by the communication bandwidth in case of sensor's using NFC IC. In [4] explains the security issues due to other technologies while in aggregating different technologies like NFC, Bluetooth and IC card onto a single platform, provides unified platforms. In paper [5] discusses the model for vehicle network operators, which allows less mobile traffic cost and has increased security. In this transfers user smart phone traffic to the network of electric vehicle, which causes to increase in the security of user privacy stored data, through embedded NFC reader and mobiles NFC application. In paper [6] studies of various authentication methodologies, it is found that NFC is vulnerable to security attacks. This can have negative impact on organization adopting NFC technology and its applications. Attacks related to confidentiality in NFC area is eavesdropping and replay attack. In [7] various algorithms for authentication and that would lead to reduce the attacks in NFC, Analytical Hierarchy Process (AHP) is a solution based on MIDAS system to secure NFC. Algorithms such as ECC and AES are the best algorithms to establish a secure channel and to prevent data corruption. In [8] different attacks are listed and scientific method to increase security is proposed. Attacks that affect integrity and data insertion, data modification and MITM attack. Attacks related to confidentiality in NFC area is eavesdropping and replay attack. Prove NFC could seem more secure and vulnerable to attacks, thereby needed little or no aid of authentication in most of use cases.

3. AES AND DES ARCHITECTURE IN NFC TECHNOLOGY

As NFC implementations are focused to speed of communications, but necessary security properties, mainly authentication between sender and recipient, are ignored. Moreover, NFC by itself does not provide encryption of data transmitted in hardware level. Security is important for electronic transactions and all use cases of NFC technology in order to prevent fraudulent data manipulation. The authentication techniques for NFC communication proposed by a number of researcher still lack some necessary security properties. In order to provide security to NFC, several techniques were proposed to provide authentication to data exchanges over NFC. Various proposed approaches deploy cryptographic techniques authentication certificates to establish secure communications between two NFC enabled devices [7]. There are typically two types of encryption algorithms namely symmetric key and Asymmetric key encryption. Symmetric cryptography uses only single key in order to encrypt and decrypt the plain text. Asymmetric algorithm uses two keys to encrypt and decrypt respectively. Hashing is one of the way for cryptographic transformation using an algorithm, but is does not use key. Among symmetric encryption this paper discusses implementation of Data Encryption Standard (DES), and Advanced Encryption Standard (AES) for NFC technology.

3.1 Data Encryption Standard in NFC

DES is one of symmetric key algorithm. DES basically uses Feistel structure for encryption and decryption process. DES uses a key length of 56 bits for encryption and decryption process. DES operates mainly in three steps. In the first step 56 bit key is given as input to the round key generator, which generates each key of 48 bit size for the 16 rounds of iterative process to generate encrypted text this is known as key scheduling i.e. second step of DES encryption. The final step is known as initial land final permutation which involves expanding permutation boxes, xor operation and substitution of boxes for final permutation to produces DES encrypted text. DES decryption process operates in reverse of the encryption method. These typical steps are followed in NFC technology for the authentication between reader and card/tag. DES authentication in NFC is presented in Figure1.

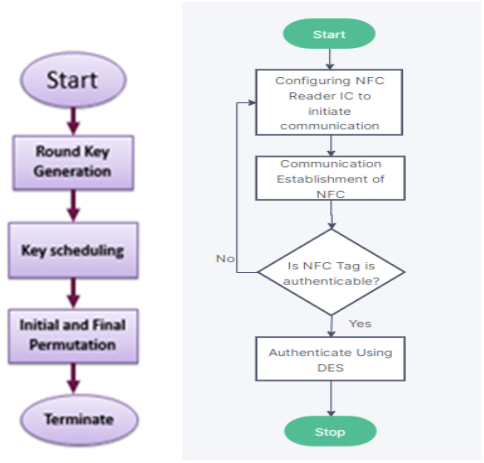

Figure 1 Flow chart of DES and DES authentication in NFC.

The above discussed DES algorithm is used to authenticate in NFC technology between reader and card/tag. Initially to establish the communication between reader and tag, reader IC being configured as defined by the NFC forum analog and digital protocol specification. Once reader detects and activates tag checks whether tag is authenticable or not, as there exist numerous tags only few are compatible for authentication. Then proceeds with DES authentication for various use cases of NFC.

3.2 Advanced Encryption Standard in NFC

AES 128 bits more compatible to most available NFC authentication tags hence 128 bits is more approachable, AES is way more secure than the DES and it can be

implementable in both software and hardware. AES 128 bits typically uses the 10 iterative rounds for both encryption and decryption process required for the authentication in case of NFC operation. Like DES method, AES also operates in the four steps in each of iterative rounds. Each round takes 128 bits of to be encrypted text and 128 bits of key which is generated by key expansion process which takes 128 bits of secret key as input. The four steps followed in each rounds are respectively are mainly byte substitution, row shifting, mix column transmission and round key addition. The decryption is the transposed process of the AES encryption method. The AES authentication method is shown in figure 2.

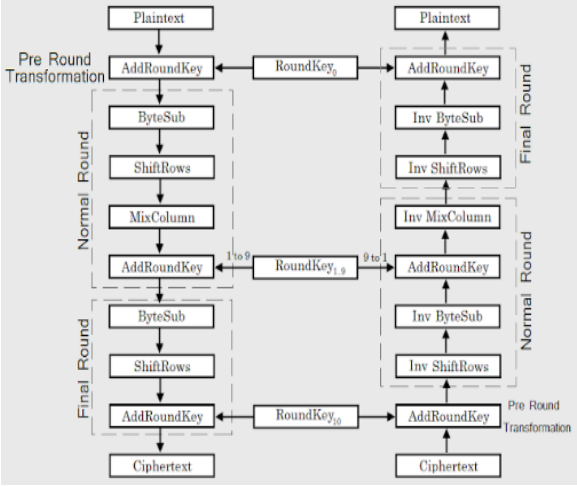

Figure 2 Flow chart of AES encryption and decryption[9].

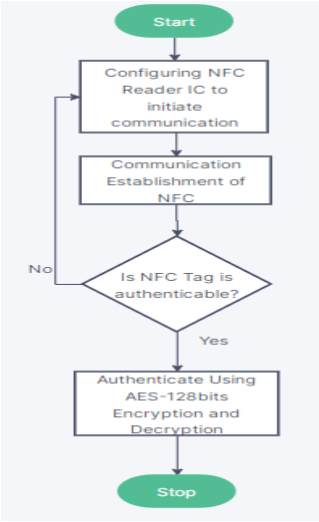

Figure 3 AES Authentication in NFC

The AES authentication between NFC reader and tag is more secure than the DES. Similarly as discussed in DES in NFC, AES authentication also works same way on top of all the data exchange operations of NFC tag as soon as the reader detects the tag in its proximity for the authentication. The authentication model of NFC is presented in Figure 4. The NFC reader issues the authentication commands to the tag, once tag responds with acknowledge to reader also sends the encrypted to the reader the reader decrypted and assures the same secret key used by both reader and tag, then reader sends encrypted data back to the tag, in similar way tag decrypts and ensures same key is used, then the authentication between tag and reader is successful.

Figure 4 Authentication model of NFC

3.3 Comparison of AES and DES in NFC

Depending on the use cases of NFC, NFC can incorporate DES or AES algorithm for the authentication between NFC reader and the NFC tag. The comparison is made based on the memory used by the both algorithm. .

Table 1: Comparison of the AES and DES in NFC Technology

DES	AES	DES
Memory used by	AES uses 13.9 KB of memory.	Memory used by DES is 16.3 KB
In order to encode one	The average number of bits	In order to encode one byte of encrypted
Key length is 56 bits	Key length is 128 bits.	Key length is 56 bits

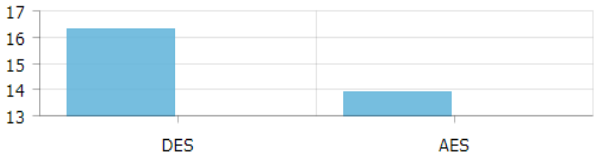

Figure 5 Memory used by security algorithm in NFC

4. CONCLUSIONS

Among various security algorithms AES and DES are more approachable in NFC technology considering both reader and tag, as most of the tags aids AES and DES authentication in almost use cases of the NFC. As enhancement for future asymmetric key algorithms like ECC are recommended as it offers more security than the symmetric algorithms such as AES and DES. To conclude the AES and DES security algorithms provide authentication in NFC Technology.

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] 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.

[3] 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.

[4] A. 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.

[5] 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.

[6] 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.

[7] 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.

[8] Ali, Ahmed H., RehamAbdellatifAbouhogail, Ibrahim F. Tarrad and Mohamed Ibrahim Youssef, “Security Analysis of NFC Technology Compared with other Mobile Wireless Technologies”, November - December 2015, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 4, Issue 6, ISSN 2278-6856

[9] Advanced Encryption Standard, https://www.researchgate.net/figure/Advanced-Encryption-Standard-AES-Algorithm_fig5_321587376