PLOS ONE

RESEARCH ARTICLE

An improved NFC device authentication protocol

He-Jun Lu[1☯]*, **Dui Liu**[2☯]

1 The School of Big Data and Artificial Intelligence, Anhui Xinhua University, Hefei, Anhui, China, **2** Security Research Institute, Hangzhou Anheng Information Technology Co., Ltd., Hangzhou, Zhejiang, China

☯ These authors contributed equally to this work.
* luhejun@axhu.edu.cn

OPEN ACCESS

Citation: Lu H-J, Liu D (2021) An improved NFC device authentication protocol. PLoS ONE 16(8): e0256367. https://doi.org/10.1371/journal.pone.0256367

Editor: Yanrong Lu, Civil Aviation University of China, CHINA

Received: April 2, 2021

Accepted: August 4, 2021

Published: August 16, 2021

Data Availability Statement: Our article belongs to Study Protocol articles. Our article does not data and the data availability policy is not applicable to our article.

Funding: This work was supported by the Project of the Quality Engineering of Education Section of Anhui Province of China (2020xfxm27, 2015ckjh117, 2016mooc190, 2017ghjc228).and the Project of the Quality Engineering of Anhui Xinhua University of China (2019sysxx03) and the Project of the Cooperation between Production and Education of Ministry of Education of the People's Republic of China (201702139041).

Abstract

Aimed at the security authentication problem between Near Field Communication (NFC) devices, this paper uses the technology of asymmetric encryption algorithm, symmetric encryption algorithm, hash function, timestamp and survival period to improve the confidentiality, performance and security of the protocol. The symmetric encryption algorithm encrypts the transmission content, while the asymmetric encryption algorithm encrypts the shared key. The whole authentication process is secure, and the key distribution is secure. The improved NFC device authentication protocol can effectively resist the brute force attack, man-in-the-middle attack and replay attack in the authentication process, it can reduce the number of message transmission in the authentication process, improve the transmission efficiency, enhance the confidentiality, integrity, non-repudiation and improve the security of NFC device authentication.

Introduction

In recent years, with the wide application of smart phones, people's life and consumption patterns have been fundamentally changed, especially in the aspect of mobile payment, which is expected to replace credit card payment and cash payments. The way of mobile payment consumption has gradually become popular and is well known and accepted by the public [1–3]. NFC technology [4] is a very common way in the process of mobile payment. This technology uses the frequency of 13.56 MHz to work within a range of 10 cm. By using the ISO/IEC 18092 standard, NFC devices can work like ordinary contactless smart cards, and is now widely used in various fields [5–8]. Because NFC contains ISO/IEC 14443 standard, relay attack is feasible [9]. At the same time, more attention is paid to its transmission efficiency in the process of NFC communication, but the security issues in the process of communication are ignored, and faced with the risk on the penetration [10], especially the defects in authentication. This paper proposes an improved, efficient and secure NFC device authentication protocol.

Symmetric encryption algorithm [11,12], asymmetric encryption algorithm [13,14], hash function [15,16] and other related technologies are used in the protocol. In the whole protocol design process, man-in-the-middle attack [17], replay attack [18], brute force attack [19], data integrity and confidentiality [20,21] and other factors are comprehensively considered. Based

Competing interests: The authors declare there are no conflicts of interest regarding the publication of this paper. There is no any commercial affiliation with Hangzhou Anheng Information Technology Co., Ltd. This does not alter our adherence to PLOS ONE policies on sharing data and materials.

on Lee et al. 's research on NFC man-in-the-middle attack [22], Ceipidor et al.' s research on NFC payment security [23], Thammarat et al. 's research on NFC security lightweight protocol [24], Tung et al.' s research on efficient NFC authentication scheme [25] and other relevant studies [26–31], an improved efficient and secure NFC device authentication scheme is proposed.

Methodology

In this paper, the protocol uses symmetric algorithm to guarantee the security of NFC device Identity (ID) and random number in the transmission process, uses public key algorithm to realize shared key distribution and message authentication, and uses hash function to verify the integrity of messages, which is divided into two stages: registration stage and authentication stage. In the registration phase, a random number is generated by the NFC device, and a random number is generated by the Authentication Server (AS). By using the two random numbers, the two-factor authentication is realized and the brute force attack is prevented. At the same time, the survival period of the NFC device issued by the authentication server and the timestamp of the authentication stage are used to prevent the replay attack. The identifiers and explanations used in this protocol are as shown in Table 1.

Registration phase

Step1 N_1—> AS: RQE1, RQS1. N_1 Sends the requests of RQE1 and RQS1 to AS.

$$\mathbf{RQE1} = \mathbf{E}_{\mathbf{puk}}\{\mathbf{K}_1\} \tag{1}$$

$$\mathbf{RQS1} = \mathbf{SK}_1\{\mathbf{IDN1}, \mathbf{Rn}_1\} \tag{2}$$

R represents the Registered stage. Q represents the Request message. E represents the use of asymmetric encryption algorithm. S represents the use of Shared Key encryption (symmetric encryption algorithm), and the number one represents the first message in the information of RQE1 and RQS1. N_1 encrypts the shared key K_1 through the public key of AS, and encrypts its own information IDN1 and random number Rn_1 through the shared key and sends it to AS to complete the shared key distribution and registration request.

Step2 AS—> N1: RPE1, RPS1. After AS receives the message from N_1, it decrypts RQE1 through its own private key to get K_1, and then RQS1 is decrypted by using K_1 to get Rn_1 and

Table 1. Identifiers and explanations used in the protocol.

Identifier	Interpretative Statement
$\mathbf{N_i}$	N is NFC device, i is NFC device number
AS	Authentication Server
E	Asymmetric Encryption Algorithm
S	Symmetric Encryption Algorithm (Shared key encryption algorithm)
puk	Public key of AS
prk	Private key of AS
$\mathbf{K_i}$	The Shared key between N_i and AS
H	Hash Encryption Algorithm
$\mathbf{Rn_i}$	The random number generated by N_i
$\mathbf{Rn_{Ai}}$	The random number generated by AS
$\mathbf{SP_i}$	The survival period of N_i
TS	Timestamps

https://doi.org/10.1371/journal.pone.0256367.t001

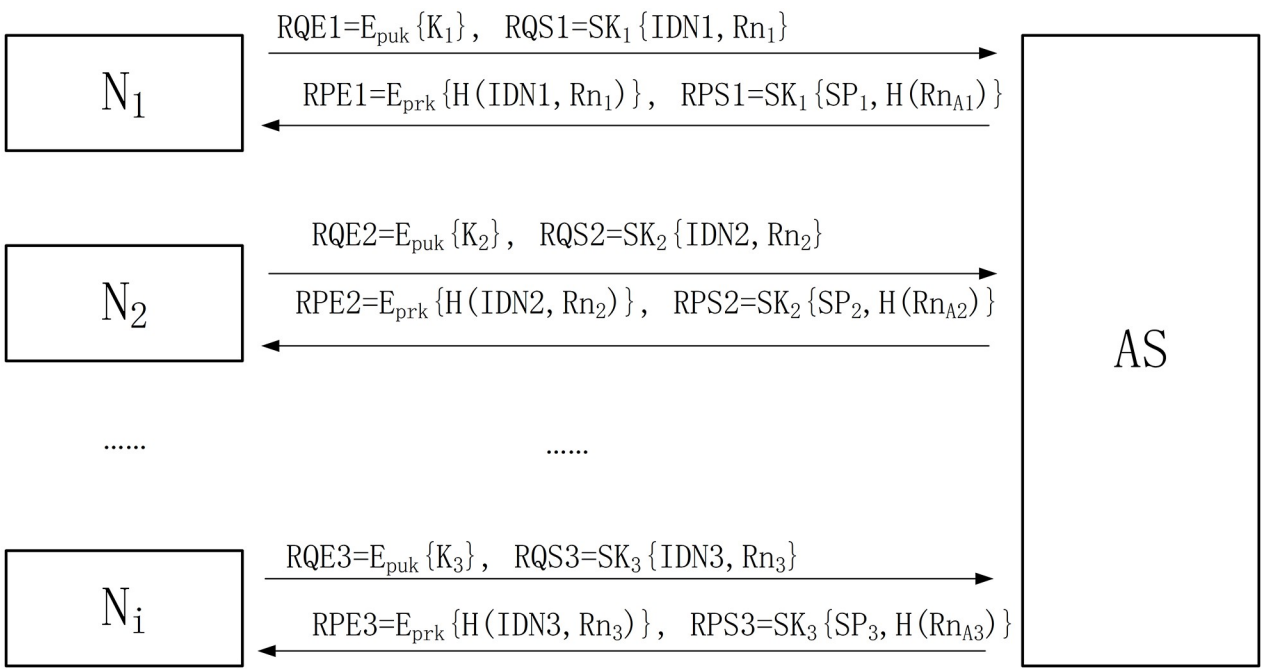

Fig 1. The working process of the registration phase.

https://doi.org/10.1371/journal.pone.0256367.g001

IDN1. After registering the IDN1 and Rn_1 of N_1 in its database, AS generates Rn_{A1} and SP_1, and sends RPE1 and RPS1 to N_1.

$$\mathbf{RPE1} = \mathbf{E}_{\mathbf{prk}}\{\mathbf{H}(\mathbf{IDN1}, \mathbf{Rn}_1)\} \tag{3}$$

$$\mathbf{RPS1} = \mathbf{SK}_1\{\mathbf{SP}_1, \mathbf{H}(\mathbf{Rn}_{\mathbf{A1}})\} \tag{4}$$

P represents the response request message in the information of RPE1 and RPS1. Rn_{A1} is the random number generated by AS. SP_1 is the survival period of N_1 device. N_1 needs to be authenticated within the SP_1, and otherwise authentication fails.

When N_1 receives RPE1 and RPS1, it decrypts RPE1 by using the public key of AS to obtain $H(IDN1, Rn_1)$, and then compares it with the $H(IDN1, Rn_1)$ generated by itself. If it is consistent, the message is indeed sent by AS and has not been changed in the transmission process. The verification is successful, then the registration stage is completed, otherwise the registration fails. The working process of the registration phase is shown in Fig 1.

Authentication phase

Step1 N1—> N2: AQS1, AQH1. N_1 sends AQS1 and AQH1 requests to N_2, where "A" represents the authentication phase in the message of AQS1 and AQH1.

$$\mathbf{AQS1} = \mathbf{SK}_1\{\mathbf{IDN1}, \mathbf{Rn}_1, \mathbf{H}(\mathbf{Rn}_{\mathbf{A1}})\} \tag{5}$$

$$\mathbf{AQH1} = \mathbf{H}\{\mathbf{IDN1}, \mathbf{Rn}_1, \mathbf{H}(\mathbf{Rn}_{\mathbf{A1}})\} \tag{6}$$

N_1 encrypts IDN1, Rn_1 and $H(Rn_{A1})$ using the shared key K_1 to generate AQS1, and at the same time carries out the hash calculation to generate the hash value AQH1 to ensure the confidentiality and integrity of the information.

Step2 N2—> AS: AQS2, AQH2. After receiving the messages send by N_1, N_2 encrypts IDN2, Rn_2, $H(Rn_{A2})$ and AQS1 with its shared key with AS to generate AQS2. At the same time, the information in AQS2 and the value of H{IDN1, Rn_1, $H(Rn_{A1})$} is used to generate the hash value AQH2 to ensure the data integrity in the transmission process. After that, the generated AQS2 and AQH2 are sent to AS.

$$\mathbf{AQS2} = \mathbf{SK_2}\{\mathbf{IDN2}, \mathbf{Rn_2}, \mathbf{H}(\mathbf{Rn_{A2}}), \mathbf{SK_1}\{\mathbf{IDN1}, \mathbf{Rn_1}, \mathbf{H}(\mathbf{Rn_{A1}})\}\} \quad (7)$$

$$\mathbf{AQH2} = \mathbf{H}\{\mathbf{IDN2}, \mathbf{Rn_2}, \mathbf{H}(\mathbf{Rn_{A2}}), \mathbf{H}\{\mathbf{IDN1}, \mathbf{Rn_1}, \mathbf{H}(\mathbf{Rn_{A1}})\}\} \quad (8)$$

Step3 AS—> N2: APS1, APE1, APE2. After receiving the request from N_2, the AS decrypts AQS2 information through K_2 and K_1, and obtains the information of IDN2, Rn_2, $H(Rn_{A2})$, IDN1, Rn_1 and $H(Rn_{A1})$. If this information does not match the data in the database, the authentication process is terminated. If it is consistent, the information in AS database is used to generate H{IDN2, Rn_2, $H(Rn_{A2})$, H(IDN1, Rn_1, $H(Rn_{A1})$}}. If it is consistent with the hash value sent by N_2, the authentication will continue, otherwise, the authentication will be terminated.

After AS verifies N_1 and N_2, it sends responses APS1, APE1, APE2 to N_2. Note that the information in APS1, APE1, and APE2 all use the information in the database of AS. TS_1 is the timestamp.

$$\mathbf{APS1} = \mathbf{SK_2}\{\mathbf{H}\{\mathbf{IDN2}, \mathbf{Rn_2}, \mathbf{H}(\mathbf{Rn_{A2}})\}, \mathbf{TS_1}, \mathbf{SK_1}\{\mathbf{H}\{\mathbf{IDN1}, \mathbf{Rn_1}, \mathbf{H}(\mathbf{Rn_{A1}})\}\}\} \quad (9)$$

$$\mathbf{APE1} = \mathbf{E_{prk}}\{\mathbf{H}(\mathbf{IDN1})\} \quad (10)$$

$$\mathbf{APE2} = \mathbf{E_{prk}}\{\mathbf{H}(\mathbf{IDN2})\} \quad (11)$$

Step4 N2—> N1: APS2, APE1. After receiving the response from AS, N_2 decrypts APE2 through the public key issued by AS to verify whether the H(IDN2) is the same as its own ID hash value to confirm whether the message comes from AS. If the verification fails, the authentication is terminated. If it succeeds, SK_2 is used to decrypt APS1 to obtain the messages of H {IDN2, Rn_2, $H(Rn_{A2})$} and TS_1. N_2 uses TS_1 to verify the validity of the message. When the verification of TS_1 passed, the H{IDN_2, Rn_2, $H(Rn_{A2})$} is calculated to be consistent with those received. If TS_1 verification fails, the authentication will be terminated. At the same time, if the verification of H{IDN2, Rn_2, $H(Rn_{A2})$} fails, the authentication will also be terminated.

When N_2 confirms that the received message is correct, APS2 and APE1 are sent to N_1.

$$\mathbf{APS2} = \mathbf{SK_1}\{\mathbf{H}\{\mathbf{IDN1}, \mathbf{Rn_1}, \mathbf{H}(\mathbf{Rn_{A1}})\}\} \quad (12)$$

$$\mathbf{APE1} = \mathbf{E_{prk}}\{\mathbf{H}(\mathbf{IDN1})\} \quad (13)$$

After N_1 receives the response from N_2, it first obtains H(IDN1) by calculating APE1 with public key, and then compares the obtained hash value with itself hash value to verify their consistency. If they are consistent, the source and integrity authentication are completed.

N_1 uses SK_1 to solve APS2 to obtain H{IDN1, Rn_1, $H(Rn_{A1})$} and then compared with the H{IDN1, Rn_1, $H(Rn_{A1})$} generated by itself using local data for matching verification. If they are consistent, the authentication is completed. Otherwise, the authentication fails and the authentication is terminated. The working process of certification phase is shown in Fig 2.

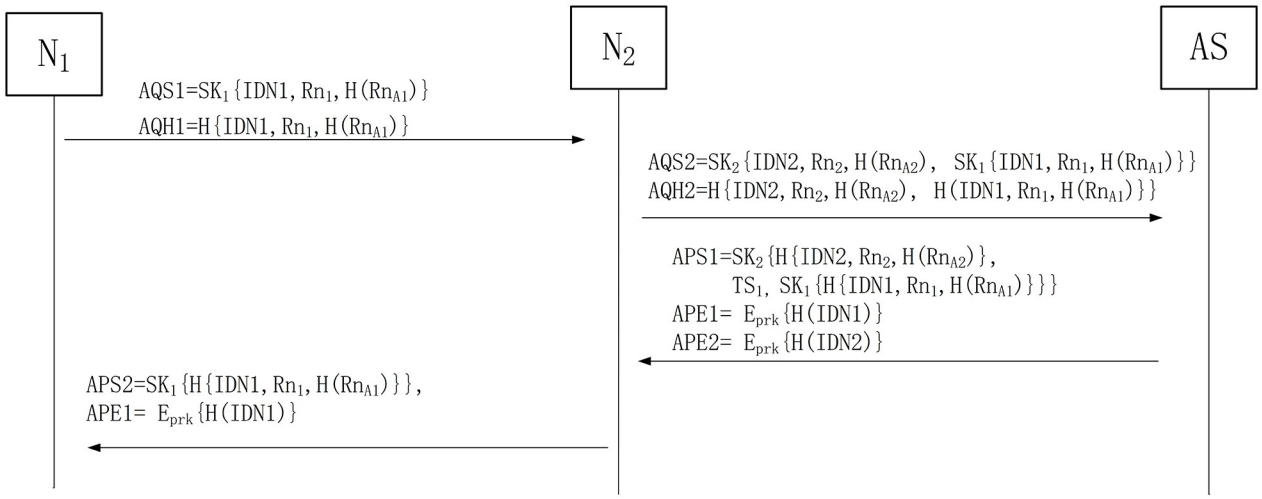

Fig 2. The working process in the authentication phase.

https://doi.org/10.1371/journal.pone.0256367.g002

Results

Prevent man-in-the-middle attacks

In this paper, ciphertext transmission is adopted. In the whole process of the protocol, including two phases of registration and authentication, the middleman cannot obtain the effective plaintext information. Suppose the middleman is located in N_1And N_2, APE1 cannot be generated, because he does not know the key of AS and the value of IDN1, so it will not pass the fourth step in the authentication phase. If the middleman is located at N_2 and AS, because he doesn't know the shared key K_2 and the private key of AS, the middleman will not generate APS1, APE1 and APE2, and TS will also be able to defend against man-in-the-middle attacks between N_2 and AS to some extent.

Prevent replay attacks

In this paper, random numbers Rn_i and Rn_{Ai}, message lifetime, timestamp and other technologies are used. Compared with the scheme proposed by Lee et al., Ceipidor et al., Thammarat et al., it can effectively achieve the purpose of preventing replay attacks.

Prevent brute force attacks

In this paper, the random numbers Rn_i generated by the NFC device and the random numbers Rn_{Ai} generated by the AS are used. At the same time, symmetric encryption, asymmetric encryption and hash encryption technologies are adopted, making brute force cracking extremely difficult. Compared with the scheme proposed by Lee et al., Tung et al., the scheme is more secure and reliable on the whole process.

Ensure data integrity

In this paper, there are corresponding hash values in each step of the registration phase and authentication phase, which can fully guarantee the integrity of the data. In the second step of authentication stage, dual hashing integrity authentication is used, which can ensure the integrity of data better than other schemes.

Ensure data confidentiality

In this paper, asymmetric algorithm is used to encrypt the key of symmetric algorithm, and symmetric algorithm is used to encrypt the data, which not only ensures the confidentiality, but also ensures the efficiency of the whole protocol. The whole process is encrypted, so that all the data obtained by the attacker are ciphertext. Compared with the scheme proposed by Ceipidor et al. and Tung et al., the data confidentiality is stronger and more secure.

Mutual authentication

In the second step of the authentication phase, AS verifies the consistency of the ID and Rn_1, Rn_{A1}, Rn_2 and Rn_{A2} by receiving requests from N_1 and N_2, and then uses the data in the local database to conduct hash calculation in response to N_1 and N_2. N_1 and N_2 use their own Rn_1, Rn_{A1}, Rn_2 and Rn_{A2} to conduct hash calculation and verify whether they are consistent and achieve the purpose of mutual authentication.

Discussion

Confidentiality and performance analysis

Compared with other schemes, this paper comprehensively uses symmetric encryption algorithm, asymmetric encryption algorithm and hash algorithm to achieve high confidentiality. In terms of message transfer operation frequency, the protocol in this paper completes the entire authentication process with the minimum message transmission times, which is efficient and safe. Comparison of confidentiality and performance analysis are shown in Table 2.

Safety analysis

This paper compares with other schemes in security aspects such as confidentiality, prevention of man-in-the-middle attack, prevention of replay attack, prevention of brute force attack, integrity, mutual authentication, etc., as shown in Table 3. It can be seen that the protocol in

Table 2. Comparison of confidentiality and performance analysis.

Operating	Our scheme	Lee et al.	Ceipidor et al.	Thammarat et al.	Tung et al.
Symmetric Encryption algorithm	8	4	-	3	-
Asymmetric Encryption algorithm	6	1	2	-	-
Hash algorithm	8	3	3	9	9
Message transmissions	6	8	7	8	7

https://doi.org/10.1371/journal.pone.0256367.t002

Table 3. Comparison of safety analysis.

Security	Our study	Lee et al.	Ceipidor et al.	Thammarat et al.	Tung et al.
Confidentiality	Yes	No	No	No	No
Preventing man-in-the-middle attacks	Yes	-	-	Yes	Yes
Prevent replay attacks	Yes	No	No	Yes	Yes
Prevent brute force attacks	Yes	-	-	Yes	Yes
Integrity	Yes	No	-	Yes	Yes
Mutual authentication	Yes	-	Yes	Yes	Yes

Note that the "-" in the table indicates that this study claims that the solution can provide this security attribute, but other studies believe that the solution still lacks this security attribute.

https://doi.org/10.1371/journal.pone.0256367.t003

this paper can complete the mutual authentication of NFC devices and ensure the security at the same time. The message transmitted in the registration and authentication stages is encrypted throughout, which is more secure than the protocol with others.

Conclusion

A secure and efficient authentication scheme between NFC devices is proposed in this paper. The whole ciphertext transmission can not only be used for communication between mobile NFC devices, but also for secure communication between NFC devices and smart cards. At the same time, the scheme uses the timestamp, survival period and other technologies to solved the man-in-the-middle attack, replay attack and other problems. The hash algorithm is used to ensure the data integrity in the transmission process. The asymmetric encryption algorithm is used to solve the problem of message source authentication and shared key distribution. The symmetric encryption is used to make the protocol more efficient. In this protocol, the number of interactive information transmission between devices is reduced as much as possible, and the messages transmitted in both the registration stage and the authentication stage are all encrypted, which makes the whole system more secure.

Author Contributions

Conceptualization: He-Jun Lu, Dui Liu.

Data curation: He-Jun Lu, Dui Liu.

Formal analysis: He-Jun Lu, Dui Liu.

Funding acquisition: He-Jun Lu.

Investigation: He-Jun Lu, Dui Liu.

Methodology: He-Jun Lu, Dui Liu.

Project administration: He-Jun Lu, Dui Liu.

Resources: He-Jun Lu, Dui Liu.

Software: He-Jun Lu, Dui Liu.

Supervision: He-Jun Lu, Dui Liu.

Validation: He-Jun Lu, Dui Liu.

Visualization: He-Jun Lu, Dui Liu.

Writing – original draft: He-Jun Lu, Dui Liu.

Writing – review & editing: He-Jun Lu, Dui Liu.

References

1. Fan W, Huang W, Zhang Z, et al. A Near Field Communication (NFC) security model based on OSI reference model. Trustcom/BigDataSE/ISPA, 2015 IEEE. 2015; 1: 1324–1328.
2. Dahlberg T, Guo J, Ondrus J. A critical review of mobile payment research. Electronic Commerce Research and Applications. 2015; 14(5): 265–284.
3. Leng S Y, Talib A, Gunardi A. Financial Technologies: A Note on Mobile Payment. Jurnal Keuangan dan Perbankan. 2018; 22(1): 51–62.
4. Coskun V, Ozdenizci B, Ok K. A Survey on Near Field Communication (NFC) Technology. Wireless Personal Communications. 2013; 71(3): 2259–2294.
5. Vedat C, Busra O, Kerem O. The Survey on Near Field Communication. Sensors. 2015; 15(6): 13348–13405. https://doi.org/10.3390/s150613348 PMID: 26057043

6. Ozdenizci B, Coskun V, Ok K, et al. A Secure Communication Model for HCE based NFC Services. 3rd International Conference on Creative Technology. 2015; 1: 1–4.
7. Tan GWH, Ooi KB, Chong SC, et al. NFC mobile credit card: the next frontier of mobile payment?. Telematics and Informatics. 2014; 31(2): 292–307.
8. Kim J, Banks A, Cheng H, et al. Epidermal electronics with advanced capabilities in near-field communication. Small. 2015; 11(8): 906–912. https://doi.org/10.1002/smll.201402495 PMID: 25367846
9. Issovits W, Hutter M. Weaknesses of the ISO/IEC 14443 protocol regarding relay attacks. 2011 IEEE International Conference on RFID-Technologies and Applications. 2011;1: 335–342.
10. Lu HJ, Yu Y. Research on WiFi Penetration Testing with Kali Linux. Complexity. 2021; 1–8.
11. Katz J, Lindell Y. Introduction to modern cryptography. Los Angeles: CRC press; 2020.
12. Elminaam DSA, Abdual-Kader HM, Hadhoud MM. Evaluating the performance of symmetric encryption algorithms. IJ Network Security. 2010; 10(3): 216–222.
13. Bhanot R, Hans R. A review and comparative analysis of various encryption algorithms. International Journal of Security and Its Applications. 2015; 9(4): 289–306.
14. Yadav AK, Singh P, Saini I, et al. Asymmetric encryption algorithm for colour images based on fractional Hartley transform. Journal of Modern Optics. 2019; 66(6): 629–642.
15. Ferguson N, Schneier B, Kohno T. Cryptography Engineering: Design Principles and Practical Applications. New Jersey: John Wiley & Sons; 2010.
16. Ahmad M, Khurana S, Singh S, et al. A simple secure hash function scheme using multiple chaotic maps. 3D Research. 2017; 8(2): 13.
17. Conti M, Dragoni N, Lesyk V. A survey of man in the middle attacks. IEEE Communications Surveys & Tutorials. 2016; 18(3): 2027–2051.
18. Ye D, Zhang TY, Guo G. Stochastic coding detection scheme in cyber-physical systems against replay attack. Information Sciences. 2019; 481: 432–444.
19. Cho JS, Jeong YS, Park SO. Consideration on the brute-force attack cost and retrieval cost: A hash-based radio-frequency identification (RFID) tag mutual authentication protocol. Computers & Mathematics with Applications. 2015; 69(1): 58–65.
20. Yu Y, Au MH, Ateniese G, et al. Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage. IEEE Transactions on Information Forensics and Security. 2016; 12(4): 767–778.
21. Bajaj S, Sion R. Trusteddb: A trusted hardware-based database with privacy and data confidentiality. IEEE Transactions on Knowledge and Data Engineering. 2013; 26(3): 752–765.
22. Lee YS, Kim E, Jung MS. A NFC based authentication method for defense of the man in the middle attack. Proceedings of the 3rd International Conference on Computer Science and Information Technology. 2013: 10–14.
23. Ceipidor UB, Medaglia CM, Marino A, et al. Kernees: A protocol for mutual authentication between nfc phones and pos terminals for secure payment transactions. Information Security and Cryptology (ISCISC). 2012; 115–120.
24. Thammarat C, Chokngamwong R, Techapanupreeda C, et al. A secure lightweight protocol for NFC communications with mutual authentication based on limited-use of session keys. Information Networking (ICOIN). 2015; 133–138.
25. Tung YH, Juang WS. Secure and efficient mutual authentication scheme for NFC mobile devices. Journal of electronic science and technology. 2017; 15(3): 240–245.
26. Singh MM, Adzman K, Hassan R. Near Field Communication (NFC) technology security vulnerabilities and countermeasures. International Journal of Engineering & Technology. 2018; 7(4.31): 298–305.
27. Ghafoorian M, Nikooghadam M. An anonymous and secure key agreement protocol for NFC applications using pseudonym. Wireless Networks. 2020; 26(6): 4269–4285.
28. Xu J, Xue K, Yang Q, et al. PSAP: Pseudonym-based secure authentication protocol for NFC applications. IEEE Transactions on Consumer Electronics. 2018; 64(1): 83–91.
29. Anusha R. Qualitative Assessment on Effectiveness of Security Approaches towards Safeguarding NFC Devices & Services. International Journal of Electrical and Computer Engineering (IJECE). 2018; 8(2): 1214–1221.
30. Bojjagani S, Sastry VN. A secure end-to-end proximity NFC-based mobile payment protocol. Computer Standards & Interfaces. 2019; 66: 103348.
31. Thammarat C. Efficient and Secure NFC Authentication for Mobile Payment Ensuring Fair Exchange Protocol. Symmetry. 2020; 12(10): 1649.