ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 3, April 2017

Bank Locker Security System using NFC

R. Anandha Praba[1], C.K. Sivaranjani[2] and V. Shanmuga Priya[3]

Assistant Professor, Meenakshi College of Engineering, Chennai, India[1]

U.G Student, Meenakshi College of Engineering, Chennai, India[2,3]

ABSTRACT: Near Field communication, abbreviated NFC is a form of contactless communication between devices like smart phones or tablets. Contactless communication allows a user to wave the Smart phone over a NFC compatible device to send information without needing to touch the devices together or go through multiple steps setting up a connection.. In recent years, a pseudonym-based NFC protocol (PBNFCP) has been proposed to withstand the security pitfalls found in conditional privacy preserving security protocol (CPPNFC). However, it still fails to prevent the claimed security properties, such as impersonation attacks against an adversary. In order to overcome these security drawbacks, a secure and efficient authentication protocol (SEAP) for NFC applications using lifetime-based pseudonyms was proposed. In addition to SEAP protocol, proposed system include OTP and Biometric (Finger print / Iris) have additional security level. A one-time password (OTP) is a password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid a number of shortcomings that are associated with traditional (static) password-based authentication. In this paper NFC, OTP and Biometric security systems are used as an access to the individual lockers. This security system is also used in Smart homes, Secured offices, Control rooms in nuclear power plants, mobile payments, ATM etc.

KEYWORDS: Near Field Communication, one-time password, biometric security.

I. INTRODUCTION

Since the rapid development of short-range wireless communication technology, there is a growing demand to design secure and efficient authenticated applications, such as secure bank lockers, smart home, ATM, control rooms in nuclear power plants, etc., in the area of consumer electronics for NFC. In the NFC environment, Trusted Service Manager (TSM) is responsible to distribute user keys to the registered users based upon the requests from the users. In this project, both NFC tags and authentication process are involved. Both NFC tags and reader follow authenticated protocol. The authenticated protocol involves only two parties, namely an initiator user and a target user. The initiator user generates a radio frequency field from NFC tags and starts the NFC interface. After receiving communication signals, the target user sends a response message to the controller and generates an OTP to the registered phone and then biometric verification is done. Due to the shared nature of wireless communication, there are several security features verified by the controller. Thus, the security is one of the prerequisite for NFC applications. Transmission capacity of NFC technology is limited as its operating frequency is 13.56 MHz with transmission speed ranging from 106 Kbps to 424 Kbps up to 4cm.

II. RELATED WORK

With the rapid development in locker applications, the NFC is expected to become very trendy technology for security services, specifically for individual bank lockers. In recent years, many researchers presented the assessment of NFC for future security systems. A public key infrastructure is used for the efficient key management and revocation among nodes, such as an initiator and target users. In this scenario, an adversary could track the user's activities by tracing its public key, and as a result, the user's privacy may be broken. In order to overcome these drawbacks, the pseudonym based technique is used in many authentication protocols including NFC. In 2013, a Conditional privacy preserving security protocol (CPPNFC) was proposed to protect the user's privacy. Later, a similar approach as presented in CPPNFC was proposed in

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 3, April 2017

2015. However, the above CPPNFC fails to prevent the impersonation attacks and they further proposed a pseudonym based NFC protocol (PBNFCP) to withstand the security drawbacks found in CPPNFC with a marginal computation cost increase. The proposed security attacks and their approach remain same as that in CPPNFC where the user cannot identify the real identity of another user. This paper further revisits PBNFCP and shows that it still fails to prevent the proposed impersonation attacks on CPPNFC against an attacker (being an insider registered user), and discusses the drawbacks of pseudonym in PBNFCP. The existing paper proposed a new secure and efficient authentication protocol (SEAP) for NFC applications using the new defined lifetime-based pseudonyms to withstand the security drawbacks found in PBNFCP. This paper proposes an advanced secure and authenticated key agreement based on NFC technology, using NFC tags, one time password, and biometric systems to withstand the security drawbacks found in existing systems.

A) EXISTING SYSTEMS

The security is done with biometric process in existing systems. But in biometric easily frauds can be done and it is not fully secured. Many of these systems will not provide proper security and the constant password is also not secure. Long distance wireless communication is also providing much confusion to identify the user. The comparison of the communication cost of the various protocols is listed below in the Table- I and the comparison of computational cost with the existing protocols are listed below in Table-II.

TABLE-I

COMPARISON OF COMMUNICATION COST

PROTOCOL	PSUEDONYM SIZE (BITS)	COMM. COST (BITS)/NO.OF. MESSAGES
Eun et al	1200	1184 (4 messages)
Kannadhasan et al	1200	1184 (4 messages)
He et al	1200	3184 (4 messages)
SEAP	624	1840 (4 messages)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 3, April 2017

TABLE-II

COMPARISON OF COMPUTATIONAL COST

PROTOCOL	COMPUTATIONAL COST
Eun et al Initiator user	$3T_{em} + 1T_{ea} + 2T_h + 2T_m + 1T_{kdf} \sim 3608T_m$
Target user	$3T_{em} + 1T_{ea} + 2T_h + 2T_m + 1T_{kdf} \sim 3608T_m$
Total cost	$6T_{em} + 2T_{ea} + 4T_h + 4T_m + 2T_{kdf} \sim 7216\ T_m$
Kannadhasan et al. Initiator user	$3T_{em} + 1T_{ea} + 2T_h + 2T_m + 1T_{kdf} \sim 3608T_m$
Target user	$3T_{em} + 1T_{ea} + 2T_h + 2T_m + 1T_{kdf} \sim 3608T_m$
Total cost	$6T_{em} + 2T_{ea} + 4T_h + 4T_m + 2T_{kdf} \sim 7216\ T_m$
He et al Initiator user	$4T_{em} + 1T_{ea} + 3T_h + 1T_{kdf} \sim 4806T_m$
Target user	$4T_{em} + 1T_{ea} + 3T_h + 1T_{kdf} \sim 4806T_m$
Total cost	$8T_{em} + 2T_{ea} + 6T_h + 2T_{kdf} \sim 9612T_m$
Proposed SEAP Initiator user	$3T_m + 1T_{ea} + 4T_h + 1T_{kdf} + 1T_{inv} \sim 3609\ T_m$
Target user	$3T_m + 1T_{ea} + 4T_h + 1T_{kdf} + 1T_{inv} \sim 3609\ T_m$
Total cost	$6T_m + 2T_{ea} + 8T_h + 2T_{kdf} + 2T_{inv} \sim 7218T_m$

NOTE: BothTABLE-I and TABLE–II are referenced from the paper **"Secure and Efficient Authenticated Protocol (SEAP)"***IEEE Transactions on Consumer Electronics, Vol.62.no.1, February 2016.*

From the above table, it shows that the Communication cost of SEAP protocol requires only 1840 bits and it is very much less when compared to the other existing protocols.

In this project, OTP is used along with SEAP protocol. This system has low computational and communication cost. The design cost of the system is also inexpensive when compared to the existing systems.

In the SEAP, both the initiator and target users require $3T_{em} + 1T_{ea} + 4T_h + 1T_{kdf} + 1T_{inv}$ operations, which is approximately $3609T_m$. Thus, the total computational cost required in SEAP is $6T_{em} + 2T_{ea} + 8T_h + 2T_{kdf} + 2T_{inv} \sim 7218T_m$.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 3, April 2017

B) PROPOSED SYSTEM

In this paper NFC is used, hence the user can be easily identified. NFC is used for short distance and hence the user can be easily is identified. Instead of constant password, the OTP is preferred to make the system more secure. All the details are stored in the DB in server for future access.

B. Contributions

The contributions of the paper are listed below:

(i) This paper analyzes and shows that the recently proposed PBNFCP fails to provide the claimed security properties, such as impersonation attacks against a malicious registered user being an attacker.

(ii) In this paper, a new secure and efficient authentication protocol (SEAP) is presented for the NFC applications using the lifetime-based pseudonyms. The proposed pseudonym and private key pair in SEAP is valid within its lifetime only. Thus, even if a pseudonym and private key pair is unexpectedly revealed to an adversary, he/she can use it within its expiry time on behalf of the corresponding user only. As a result, the vulnerability in this case is limited to the corresponding user only, whereas in PBNFCP and CPPNFC protocol causes to the impersonation attacks to any legitimate user in the system when the identity of that user is known to the adversary. Moreover, the size of the proposed pseudonym in SEAP is significantly reduced.

(iii) The rigorous informal security analysis shows that SEAP is secure against possible well known attacks including the impersonation and man-in-the-middle attacks. In addition, the simulation results for the formal security verification using the widely accepted AVISPA tool shows that SEAP is secure against the passive and active attacks.

(iv) SEAP significantly reduces the computation and communication costs, and also provides more security functionalities as compared to the related existing protocols.

(v) Due to efficiency and more security functionalities, SEAP is very suitable for the short-range wireless communication applications, such as secured locker access, service discovery, e-payment, ticketing, and mobile healthcare systems, etc., in the area of the consumer electronic devices in the NFC environment.

(vi) In addition to this, One-time password (OTP) and Biometric systems are also used for additional security purposes.

C. Organization of the paper

The rest of the paper is sketched as follows. In Section II, the block diagram of this paper is figured. The various blocks of this diagram and its working are explained in the following sections. The performance comparison with related scheme is described in section VI. Finally, the paper is concluded in Section VII.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 3, April 2017

II. BLOCK DIAGRAM

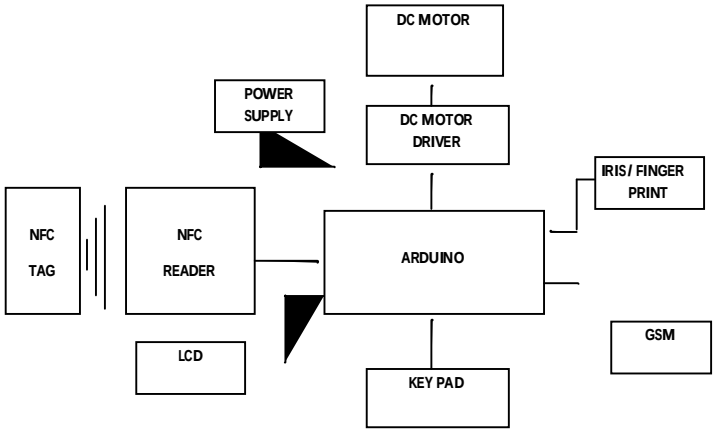

Fig.1. Block diagram of Bank security system using NFC

III. NEAR FIELD COMMUNICATION

Near-field communication (**NFC**) is a short-range wireless communication technology that enables communication between two devices that either touch or are momentarily held close together. NFC-based communication between two devices is possible when one device acts as a reader/writer and the other as a tag. NFC tag is a thin simple device containing antenna and small amount of memory. It is a passive device, powered by magnetic field. Depending on the tag type the memory can be read only, re-writable, and writable once. NFC reader is an active device, which generates radio signals to communicate with the tags. The reader powers the passive device in the case of passive mode of communication.

The technology behind NFC allows a device, known as a reader, interrogator, or active device, to create a radio frequency current that communicates with another NFC compatible device or a small NFC tag holding the information the reader wants. Passive devices, such as the NFC tag, store information and communicate with the reader but do not actively read other devices.

Peer-to-peer communication through two active devices is also a possibility with NFC. This allows both devices to send and receive information. Both businesses and individuals benefit from near field communication technology.

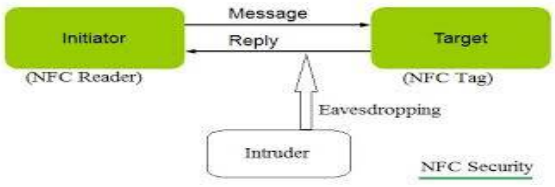

Fig.2. Communication between NFC tag and NFC Reader

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 3, April 2017

IV. GENERATION OF ONE TIME PASSWORD

OTP generation algorithms typically make use of pseudo randomness or randomness, making prediction of successor OTPs by an attacker difficult, and also hash functions, which can be used to derive a value but are hard to reverse and therefore difficult for an attacker to obtain the data that was used for the hash. This is necessary because otherwise it would be easy to predict future OTPs by observing previous ones. Concrete OTP algorithms vary greatly in their details. Various approaches for the generation of OTPs are listed below:

- Based on **time-synchronization** between the authentication server and the client providing the password (OTPs are valid only for a short period of time)
- Using a mathematical **algorithm** to generate a new password **based on the previous password** (OTPs are effectively a chain and must be used in a predefined order).
- Using a mathematical **algorithm** where the new password is **based on a challenge** (e.g., a random number chosen by the authentication server or transaction details) and/or a counter.

There are also different ways to make the user aware of the next OTP to use. Some systems use special electronic security tokens that the user carries and that generate OTPs and show them using a small display. Other systems consist of software that runs on the user's mobile phone. Yet other systems generate OTPs on the server-side and send them to the user using an out-of-band channel such as SMS messaging.

V. BIOMETRIC SYSTEMS

Biometrics refers to metrics related to human characteristics. Biometrics authentication (or realistic authentication) is a form of identification and access control. It is also used to identify individuals in groups that are under surveillance. The first time an individual uses a biometric system is called *enrollment*. During the enrollment, biometric information from an individual is captured and stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrollment. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is to be robust. The first block (sensor) is the interface between the real world and the system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired. The second block performs all the necessary pre-processing: it has to remove artifacts from the sensor, to enhance the input (e.g. removing background noise), to use some kind of normalization, etc. In the third block necessary features are extracted. This step is an important step as the correct features need to be extracted in the optimal way. A vector of numbers or an image with particular properties is used to create a *template*. A template is a synthesis of the relevant characteristics extracted from the source. Elements of the biometric measurement that are not used in the comparison algorithm are discarded in the template to reduce the file size and to protect the identity of the enrollee.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 3, April 2017

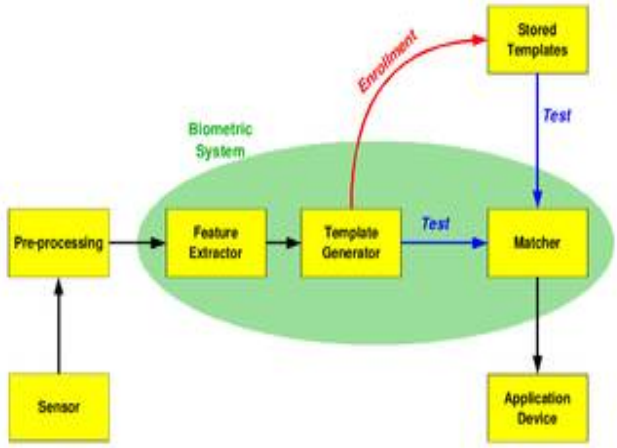

Fig.3. Block diagram of Biometric system

During the enrollment phase, the template is simply stored somewhere (on a card or within a database or both). During the matching phase, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). The matching program will analyze the template with the input. This will then be output for any specified use or purpose (e.g. entrance in a restricted area). Selection of biometrics in any practical application depending upon the characteristic measurements and user requirements. In selecting a particular biometric, factors to consider include, performance, social acceptability, ease of circumvention and/or spoofing, robustness, population coverage, size of equipment needed and identity theft deterrence. Selection of a biometric based on user requirements considers sensor and device availability, computational time and reliability, cost, sensor size and power consumption. In this paper, the finger print sensors are preferred for low cost applications and iris recognition scanners are preferred for high security applications.

VI. PERFORMANCE COMPARISON WITH RELATED SCHEMES

This section analyzes the performance of the proposed system, and compares it with the features of existing systems. It also gives a detailed description about the specific features of the proposed model.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 3, April 2017

TABLE III

COMPARSION OF EXISTING AND PROPOSED SYSTEM FEATURES

EXISTING SYSTEM	**PROPOSED SYSTEM**
Private Key is used.	NFC tag is used.
Constant password is used.	OTP (One Time Password) is used.
User cannot easily identify the real identity of another user.	Unauthorized user can be easily identified due to NFC technology.
High computation and Communication costs.	Low computation and Communication Costs.
Less secure.	Highly secure.

VII. CONCLUSION

The earlier proposed protocol PBNFCP is first analyzed and then shown that it is vulnerable to two kinds of impersonation attacks. A novel secure and efficient authentication protocol (SEAP) for NFC applications is proposed using the lifetime-based pseudonyms with significantly low computation and communication costs as compared to existing related authentication protocols. This also has the drawback of impersonation attacks. In order to overcome this drawback, three security levels such as NFC,OTP and Biometric are used in this system. Through the rigorous security analysis, this paper shows that it is secure against possible known attacks including the impersonation attacks found in PBNFCP and SEAP protocol. Thus, this system provides high security along with low computation and communication costs as compared to the related existing protocols.

VIII. FUTURE ENHANCEMENTS

By the integration of IOT (Internet of Things) concept, it's possible to access the system from remote main station. All login and logout details are stored in a temporary storage area for future use. Instead of OTP passwords, the combination of both Static and OTP pseudonyms can also be used. The usage of Smart Cameras in Controller will be an additional security to this system in future, for capturing the images of an unauthorized user.

This locker security system also used in various places in future such as Smart homes, Secured offices, Control rooms in nuclear power plants , ATM. It is also used in Mobile payments

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 3, April 2017

REFERENCES

1. Vanga odelu, Ashok Kumar and Adrijit Goshwami, "Secure and Efficient Authentication Protocol (SEAP) for NFC Applications Using Pseudonyms", *IEEE Transactions on Consumer Electronics*, Vol.62, No.1, February 2016.
2. Jayesh B Mahajan, Bhagwat Kakde, and Anurag Rishishwar, "Mall Shopping System Using NFC," *International Journal of Scientific and Research Publications*, Volume 5, Issue 11, Nov.2015.
3. V. Odelu, A.K. Das and A Goshwami, "A Secure biometrics-based multi-server authentication protocol using smart cards", *IEEE Trans.Inf.Forensics Security*, Vol.10, No.9, June 2015.
4. W. Lumpkins and M. Joyce, "Near-Field Communication: It Pays: Mobile payment systems explained and explored,"*IEEE Consum.Electron. Mag.*, vol.4, no.2, pp.49-53, April. 2015.
5. D. He, N. Kumar, and J. H. Lee, "Secure pseudonym-based near field communication protocol for the consumer internet of things,"*IEEE Trans. Consumer Electron.*, vol. 61, no. 1, pp. 56-62, Mar. 2015.
6. S. Kannadhasan, M. Isaivani, and G. Karthikeyan, "A Novel Approach Privacy Security Protocol Based SUPM Method in Near Field Communication Technology,"*in Proc. Artificial Intelligence and Evolutionary Algorithms in Engineering Systems*, Kumaracoil, India,vol. 324, pp. 633-643, Nov. 2014.
7. H.Eun, H. Lee, and H.*Consumer Electron.*, vol.59, no. 1, pp.153-160, Apr. 2013.
8. Juniper Research, "NFC Mobile Payments & Retail Marketing-Business Models & Forecasts 2012-2017," May 2012.
9. V. Coskun, K. Ok, and B. Ozdenizci, *Near Field Communication (NFC): From Theory to Practice*, London: ISBN: 978-1-1199-7109-2, Feb. 2012.

BIOGRAPHY

R.Anandha Praba received her B.E. degree in Electronics and Communication Engineering from Anna University, Chennai and M.E. degree in Applied Electronics from Anna University, Chennai. She is working as Assistant Professor in the Electronics and Communication Engineering Department, Meenakshi College of Engineering, Chennai.

C.K. Sivaranjani and V. Shanmuga Priya is doing their final yearin the Electronics and Communication Engineering Department, Meenakshi College of Engineering, Chennai.