International Journal of Electrical and Computer Engineering (IJECE)
Vol. 8, No. 2, April 2018, pp. 1214~1221
ISSN: 2088-8708, DOI: 10.11591/ijece.v8i2.pp1214-1221

Qualitative Assessment on Effectiveness of Security Approaches towards Safeguarding NFC Devices & Services

Anusha R., Veena Devi Shastrimat V.
Department of Electronics & Communication Engg, NMAM Institute of Technology, NITTE, India

Article Info

Article history:

Received Jul 15, 2017
Revised Jan 3, 2018
Accepted Jan 7, 2018

Keyword:

Mobile security
Near field communication
RFID
Security
Wireless security

ABSTRACT

The increasing pace in the wireless communication taking momentum in the market of commercial application where a significant trade-off between user-experience and security demands exists. The Near Field Communication or NFC is one such communication trend which is effectively adopted by the user worldwide to make touchless operation using their mobile device. Although, it is claimed that NFC incorporates some of the standard encryption but existing researchers fails to prove that their electromagnetic signals are snot so difficult to compromise to result in collateral damage to user's resources. Thus, there exist research work towards strengthing security system, but there is yet to report on any standard security protocol or framework to ensure the highest resiliency. This paper provides a comprehensive visualization towards the effectiveness of existing research approaches to formulate the research trend and gap.

Corresponding Author:

Anusha R.,
Department of Electronics & Communication Engg,
NMAM Institute of Technology,
NITTE, India.
Email: anu4research@gmail.com

1. INTRODUCTION

NFC or Near Field Communication is mainly known for its wireless mechanism to transmit/exchange data using high frequency (13.56 MHz) within shorter ranges (nearly 10 cm) of communicating devices [1]. An electromagnetic field is being generated by a small NFC chip residing within the communicating device that is captured by other NFC device (called as tags) that could be anything right from smart poster to the NFC-based point of sale device. The information is exchanged from the NFC tags to the communicating devices. Normally, the transmission speed of data is very fast in NFC devices ranges from 106-424 kbps. It can also be said that NFC is an enhanced version of legacy Radio Frequency Identification RFID system that amalgamates both readers as well as smartcard interface in one communication device [2]. However, the fact is NFC is very much different from RFID as well as any other wireless standards. The usage of NFC has been evidently seen in some recent applications, e.g., Apple Watch, Samsung Pay, etc., which are mainly smartphone devices. NFC differs from any other communication technologies in smartphones by its significantly shorter set up time which 1/10 seconds [3]. This phenomenon also assists in incorporate good security in NFC devices from being less vulnerable in the crowded location which is not the case with Bluetooth and other Wireless Communication system [4]. The significant advantage of NFC is that it doesn't have any dependencies on power (i.e., battery). Even if the phone is in off mode, the NFC application is still functional. However, there are some obvious security concerns with the usage of NFC. The *first security concern* is NFC allows one-touch execution which makes the device very much vulnerable as it stores lots various credential information in the mobile devices in case of illegitimate intercepting of payment process [5]. An advance security mechanism, e.g., biometrics, tokenization, hybridizing approaches are still under the roof of research [6]. The *second security concern* in

NFC is used for heterogeneous platform for making the payments, which makes lot of differences in security performance even if they run same application. The *third security concern* with NFC is that it has all the possibility of catching wrong signals. This means that as RFID is the backbone of NFC so whenever there is any form of electromagnetic signals, it alerts the NFC apps which may not be the desired tag in real sense. Apart from all the above security concern, eavesdropping is another critical security concern in NFC that takes place when the signal is illegally intercepted by the third party when two NFC devices are communicating. In such condition, there is all the possibility that confidential information within the mobile device will be silently be accessed by the intruder without even knowledge of owner of the device. This problem of eavesdropping give rise to another potential problem, i.e., data corruption [7] where the adversary changes or do some sort of tampering with the eavesdropped data. At present, the researchers have presented some valuable contribution towards safeguarding the communication in NFC-based devices. However, still, there is no reported case of strength or effectiveness of any existing approaches of security in the area of NFCs. Therefore, this manuscript contributes towards exploring the effectiveness of existing research approaches of securing NFCs. Section 1.1 discusses the background and brief highlights of research problems identified are addressed in Section 1.2 while proposed solution is presented in 1.3. Section 2 discusses fundamental information about NFC followed by discussion of existing research contribution along with their addressed problems, applied techniques, advantages and limitation in Section 3. Existing research trend highlighting most frequently used techniques for offering security features in NFCs is discussed in Section 4 followed by highlights of significant research gap from existing research contribution in Section 5. Finally, conclusion is briefed in Section 6.

1.1. Background

This section briefs the existing studies that have been carried out towards addressing the security issues in NFC-based device, applications, and services. The work of Jianli et al. [8] designed an security system model for NFC device using two dimensional code encryption and found that it provides the boot password for the mobile phone. Senthil Kumar and Mathivanan [9] presented the password protected NFC card which provides the personal code and is secure one. Paramsivam and Arivazhagan [10] presented the NFC based digital technique to mitigate the coin shortage issue.

Instead of various manuscripts highlighting about security threats of NFC, there is only two standard literature that has reported security challenges in NFC. The work carried out by Chen et al. [11] have presented a discussion of different forms of threats in NFC and briefed that majority of the attacks in NFC are generated from card emulation mode (denial of service, relay attack) as well as reader-writer mode (ticket cloning, phishing). Similarly, we have reviewed the work presented by Nyikes [12] who have discussed significant security challenges associated with RFID that is an essential backbone of NFC architecture. However, apart from these, there is little standard manuscript towards highlighting the security emergence of NFCs.

1.2. Research Problem

With upcoming communication and entertainment devices going much advance in wireless communication system, the incorporation of NFC is increasing day by day. From the prior section, it is now known that there is few number of standard review-based literature aimed towards exploring the effectiveness of existing security approaches of NFC. At the same time, there is presence of very less number of literatures that talk about implementation scheme of strengthing the security of NFCs. Hence, the biggest research problem is that it is not necessary that adoption of cryptographic algorithm that has proven its robustness in other wireless field needs to be equally of similar cadre in NFCs. In fact, usage of elliptical curve causes various computational complexities that have never been found discussed in any of the existing research studies.

1.3. Proposed Solution

The study focuses on discussing the existing techniques and approaches for strengthing the security features of NFC devices, application, and services. At present, there are very much scattered form of literature with diverse security techniques; it is quite challenging to explore the study effectiveness. Therefore, we filter only manuscripts from reputed and standard publishers that have been published during 2010-2017. The inclusion criteria of the existing studies are only security or cryptographic based approaches in NFC whereas the exclusion criteria are other generic RFID based security system. It is because NFC uses a specific RFID structure that is very different from generic RFID structure. The proposed study essentially explores the effectiveness of existing security approaches of the NFC and also discusses the specific problems that have been focused on by the researchers. The proposed system also explores various techniques applied to solve such problems followed by brief identification of the limitation of each of the

significant approaches of existing system. After reviewing the research trend, the proposed system also contributes to extract the research gap from the existing security approaches in NFC.

2. SECURITY CHALLENGES IN NFC

The NFC-based application suffers from various security challenges. In present time, a standard known as NFC-SEC is used for securing NFC-devices from adversaries by incorporating Secured Channel Services (SCH) and Shared Secret Service (SSE) [13]. The integrity and confidentiality are maintained by SCH with the aid of generated key from a module called as SSE. Adoption of Elliptical Curve Cryptography and Diffie Hellman is used for developing a key agreement between two NFC devices that demands both private and public keys. The core modules of NFC environment are Trusted Service Manager (TSM) and Secure Element (SE). TSM plays the role of certificate authority while SE is all about safeguarding the valuable data. It is also believed that SE offers higher degree of tamper resistance along with the trusted third party, i.e., TSM. Majority of the security issues arises in the Logical Link Control Protocol in standard architecture of NFC devices (Figure 1). It has been seen that majority of the NFC application uses mobile payment system where both the forms of keys are mandatorily required to be constructed on the basis of elliptical curve cryptography.

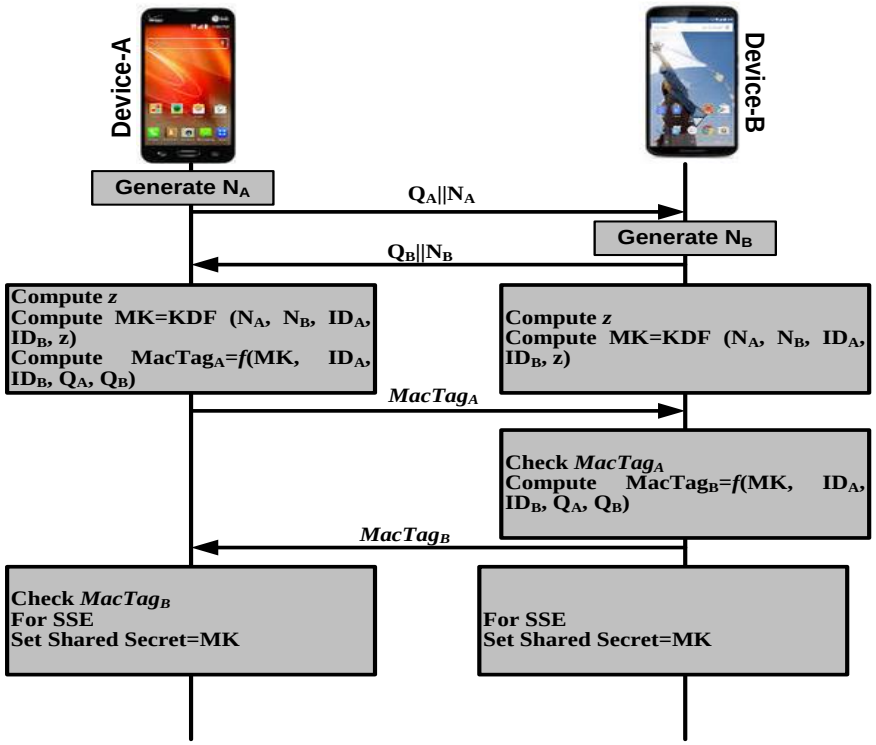

Figure 1. Working Principle of NFC-SEC

A public key in compressed form, as well as random number, is concatenated for forwarding from user 1 to user-2 who generates another random number. Applying elliptical curve, the significant point is considered as the secret key of different value for both users. A secret key is extracted using the identity of devices, arbitrary numbers, and confidential value. A new NFC tag is generated and exchanged with each other for validating the secret key. The public key, identity-based information, and secret key are used for generating such NFC tags. The identification of the NFC can be carried out using identity, but they can only access the partial information about it. The updating operation of NFC is independent of any messages or its connectivity. One of the biggest challenging factors here is the usage of the public key which is fixed for the devices. Hence, an adversary can easily collect it from the history of communication. For this purpose, NFC-based devices and services suffer from different ranges of applications, e.g., man-in-middle attack, eavesdropping, data corruption, data modification, data insertion, etc. Although some of the suggestion

mechanism to safeguard intrusions on NFC is disabling mobile NFC when it is not required, adoption of secure socket layer, and using password locking system do exist, but presence of lethal adversaries have outrun the existing security system.

3. EXISTING SECURITY APPROACHES IN NFC

This section discusses about the existing security approaches towards NFC. Usage of homographic encryption system is seen implemented most recently by Diaz et al. [14] in order to secure the communication system of airport exclusively focusing on the baggage control system. Another recent work has been carried out by Majumder et al. [15] have discussed a novel cloaking system to secure the electronic payment system, e.g., Samsung pay, google wallet, PayPal, etc. The paper has also discussed about existing research work towards payment system on NFC along with their verification techniques. Similar direction of research towards payment-based application was carried out by Park et al. [16] Madhoun [17] where the authors have presented a mutual authentication mechanism over NFC enabled mobile device. The technique implements lattice-based convolution scheme for multiplication operation. Study towards mutual authentication scheme was also carried out by Fan et al. [18], [19] that implements logical operation of XOR for resisting denial-of-service attacks. Adoption of key management towards securing NFC-based devices was seen in the work presented by Jin et al. [20] where the authors have presented a key agreement scheme that ensures energy efficiency using software-defined radio testbed. Literatures have also witnessed the usage of pseudonyms towards secure authentication of NFC application as seen in the work carried out by Odelu et al. [21]. The technique presented by the author uses simulation-based scheme to ensure the reduced size of the pseudonyms. The presented technique has proved that existing pseudonym-based approaches are all shrouded with security loopholes towards addressing impersonation attacks. This technique is claimed to offer similar form of security performance for a longer duration of time. The work carried out by Ozdenizci et al. [22] has introduced a tokenization scheme for ensuring identity verification of NFC services using host card emulation. The technique also implements a unique token generation process followed by encrypted storage of data. Rios et al. [23] have presented a technique where the assessment outcomes of any examination could be rendered anonymous with an integration of QR code and NFC applications. Eldefrawy and Khan [24] have presented a scheme that supports validation mechanism for banknote using NFC device where the RFID is inserted within the banknote for performing authentication. Adoption of pseudonym towards securing the communication system was seen in the work carried out by He et al. [25], where the authors have focused on addressing privacy problems. The authors have investigation prior technique and performed a security analysis with respect to anonymity of user, mutual authentication, and security of session key. Rasua et al. [26] have introduced a protocol for analyzing attacks on the wireless network using experimental methodology. Ren et al. [27] have discussed various studies towards usage of NFC application that uses barcode. The author has also discussed the possible challenges encountered in an NFC-based application that uses barcodes.

Literature has witnessed that usage of mobile payment based application in more in NFC technologies. One such study was introduced by Chang [28] that developed a unique authorization control for the user's mobile device. An application environment is created for assisting NFC-based mobile payment system. The technique also introduces a model for access control where different policies are maintained for judging the access request of a user. Usage of asymmetric encryption on NFC application was witnessed in work carried out by Plos et al. [29] using hardware profiles of RFID. The encryption was carried out using Advanced Encryption Standard (AES), digital signatures, and Elliptical Curve Cryptography (ECC). The complete implementation has been carried out in hardware platform where different cryptosystems were assessed. Study towards protecting privacy in NFC-based application was seen in the work of Eun et al. [30] where conditional approach is specified. The authors have implemented multiple pseudonyms for ensuring optimal privacy. Gummeson et al. [31] for addressing security breaches on the user NFC enabled mobile devices. The study has implemented a design of form-factor that is adhered to the mobile device meant for jamming any form os illegitimate communication. At the same time, the authors have also ensured energy efficient mechanism towards mobile device battery. There is various applications that has the supportability of assisting in peer-to-peer based communication system in literature. The works carried out by Nandakumar et al. [32] have implemented an acoustic-based approach for truncating the dependencies on the NFC-based mobile hardware. The authors have also assessed the security effectiveness using different forms of attacks. The study carried out by Matos et al. [33] has presented a technique for securing various hotspots for the NFC devices. As such hotspots are accessible to many users; therefore chances are more for the intrusion, e.g., eavesdropping, man-in-middle attack. The architecture presented offer passive authentication using public keys as well as effective implementation. The next section tabulates the summary of existing approaches of securing NFC devices as shown in Table 1.

Table 1. Summary of Existing Approaches

Authors	Problems	Technique	Advantage	Limitation
Diaz et al. [15]	Baggage control in airport	Paillier Cryptosystem	Supports forward secrecy	Consumes time to read/write NFC tags
Majumder et al. [16]	e-payment on mobile (using biometric)	Prototyping	Simplified usage	No extensive analysis of outcomes
Park et al. [17]	Mutual authentication in	Lattice-based	Computationally	No numerical analysis
Madhoun [18]	NFC-payment	convolution	efficient	
Fan et al. [19][20]	Denial of service attack	XORing, mutual authentication	Resistive against synchronous attack	Time complexity not discussed
Jin et al. [21]	Eavesdropping, passive attack	Simulation, experimental	Energy-efficient	Lacks Complexity analysis
Odelu et al. [22]	Authentication	Pseudonyms, ECC, Signature	Resist impersonation attack	Introduces complexity
Ozdenizci et al. [23]	Access Control	Tokenization	Ensure data protection	No numerical analysis
Rios et al. [24]	Anonymity in transmission	QR Code, experimental	Simplified architecture	Lacks Complexity analysis
He et al. [25]	Privacy issues, impersonation attack	Pseudonym, signature	Simple implementation	Increased computational cost
Rasua et al. [26]	Distance fraud, mafia attack	Analytical, experimental	Maintains forward & backward secrecy	Size of key increase complexity
Ren et al. [27]	Studying NFC based application	Explorative study	Good theoretical information	Doesn't discuss limitation of existing
Chang [28]	Access control	XML encryption, signature	Supports non-repudiation	Lacks Complexity analysis
Plos et al. [29]	Security in NFC device	Experimental, asymmetric encryption, ECC, signature	Practical realization	Narrowed scope of study
Eun et al. [30]	Device security	Multiple pseudonym	Lesser overhead	No extensive numerical analysis
Gummeson et al. [31]	Device security	Experimental, Jamming malicious interaction	Successfully defend many malicious attacks, energy efficient	Doesn't address the complexity associated
Nandakumar et al. [32]	Securing peer-to-peer	Acoustic secrecy	Minimizes eavesdropping, free from	No benchmarking
Matos et al. [33]	Authenticating hotspots	Experimental, passive and dynamic authentication	Reduced authentication time	No benchmarking

4. RESEARCH TREND

The existing research work towards addressing security problems in NFC-based application is not much in number. We explored that there are only 35 journals, 287 conference papers, two early access articles published from 2010 to 2017. Figure 2 highlights that existing research trends are more inclined towards usage of cryptographic protocol, pseudonyms, mutual authentication, and privacy preservation based approaches to offer security features in NFC-based application. It was also explored that majority of the security approaches have mainly focused on mobile payment system using either barcode based or QR code based authentication mechanism. However, usage of cryptographic-based approaches are mainly found to be using elliptical curve cryptography, digital signatures, symmetric/asymmetric encryption.

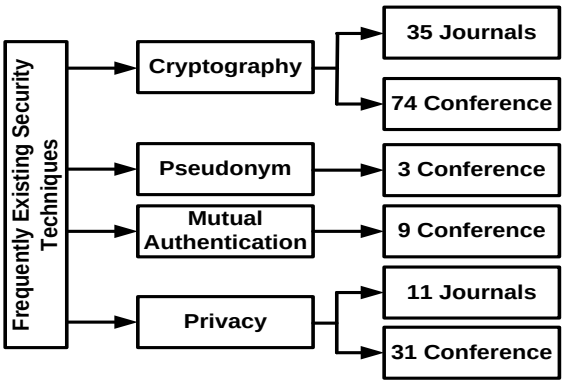

Figure 2. Existing Research Trends

5. RESEARCH GAP

Following are the significant research gap identified after reviewing the existing security approaches in NFC-based applications:

a. Incompatible Encryption Usage: Majority of the existing system make use of encryption mechanism that is not typically designed to handle the faster authentication demands of NFC-based application. Usage of pseudonyms, symmetric/asymmetric encryption, Elliptical Curve Cryptography consumes good amount of resources and is highly iterative process. Hence, its applicability towards RFID based authentication in NFC calls for extremely faster authentication process, which is missing in existing research approaches.

b. Complex Cryptographic Usage: Existing cryptographic technique towards securing NFC devices have higher key sizes and complex memory management that causes delay during the authentication process. Adoption of lightweight algorithmic approach is entirely missing from the existing literature towards cost-effective computational processing of security algorithms in NFC devices./

c. Symptomatic approach: The existing security approaches are highly symptomatic in its security characteristics that will not be applicable if the investigation environment is altered as well as the adversary is altered. Moreover, existing approaches don't offer resiliency towards various other forms of lethal threats, e.g., key compromisation issue, replay attack, card emulation, compromised gateway, etc.

d. Fewer significant studies: At present research work towards securing NFC based applications are not even more than 100 journals since last seven years. On the other side, the approach of cryptography has been making highly progressive features in network and security, but very few of them have been found towards NFC. Majority of the work have used more or less similar security strategies. Another issue is that there has been considerably less number of consideration of applications. It has to be known that NFC applications are highly vast and every application demands different form of security.

e. Less Work being Benchmarked: At present, none of the existing research-based approaches are found to be benchmarked or being compared with standard security protocols in NFC or RFID based applications. Existing studies also don't emphasize on the computational complexity associated with the key management. Hence, there is no standard evidence of any significant algorithm that has been proven to be highly resistive against malicious threats in NFC-based applications and services.

6. CONCLUSION & FUTURE WORK

After reviewing the existing research-based approaches in NFC for strengthing the security feature, we concluded that there are problems associated with the usage of cryptographic algorithm in NFC. It is quite obvious that usage of complex cryptographic policies may lead to potential encryption, which is good for security, but it may not offer better communication performance too for much upcoming application that requires streaming of data.

Therefore, our next level of research work will focus on applying certain lightweight cryptographic approaches, e.g., the hummingbird that has never been tried for securing communication in NFC. As hummingbird harnesses the potential of both stream and block cipher, so there is a fair chance of minimizing any form of computational complexity associated with cryptographic algorithm in NFC.

REFERENCES

[1] Tom Igoe, Don Coleman, Brian Jepson, "Beginning NFC: Near Field Communication with Arduino, Android, and PhoneGap," O'Reilly Media, Inc, 2014
[2] Agus Kurniawan, "Near Field Communication (NFC) for Embedded Applications," PE Press, 2015
[3] Dominique Paret, "Antennas Designs for NFC Devices," John Wiley & Sons, 2016
[4] Sheli McHugh, Kristen Yarmey, "Near Field Communication: Recent Developments and Library Implications," Morgan & Claypool Publishers, 2014
[5] Jakob Harb, "Acceptance and Success Factors for NFC-Mobile-Payment in South Korea," In comparison to Austria and Taiwan, GRIN Verlag, 2016
[6] Dan Schatt, "Virtual Banking: A Guide to Innovation and Partnering," John Wiley & Sons, 2014
[7] Michael Roland, "Security Issues in Mobile NFC Devices," Springer, 2015
[8] Jianli, Chu, Sun Yongdao, and Liu Xia, "The Research of Mobile phone Entrance Guard System Model based on the Encryption Two-dimensional Code," *Indonesian Journal of Electrical Engineering and Computer Science* 11.9 (2013): 5284-5292.

[9] Kumar, Senthil, and V. Mathivanan, "NFC Secured Offline Password Storage," *Indonesian Journal of Electrical Engineering and Computer Science* 8.3 (2017).
[10] Paramasivam, E., and D. Arivazhaga. "NFC Based Digital Innovation Technique to Eliminate Coin Shortage Problem," *Indonesian Journal of Electrical Engineering and Computer Science* 8.3 (2017): 651-653.
[11] Cheng-Hao Chen, Iuon-Chang Lin, Chou-Chen Yang, *"NFC Attacks Analysis and Survey"*, IEEE Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 2014
[12] Zoltán Nyikes, *"Information Security Issues of RFID"*, IEEE 14th International Symposium on Applied Machine Intelligence and Informatics, 2016
[13] "Security, NFC-SEC", http://www.ecma-international.org/activities/Communications/tc47-2008-089.pdf, Retrived 8th July, 2017
[14] Néstor Álvarez-Díaz, Pino Caballero-Gil, andMike Burmester, "A Luggage Control System Based on NFC and Homomorphic Cryptography", *Hindawi-Mobile Information Systems*, 2017
[15] A. Majumder, J. Goswami, S. Ghosh, R. Shrivastawa, S. P. Mohanty and B. K. Bhattacharyya, "Pay-Cloak: A Biometric Back Cover for Smartphones: Facilitating secure contactless payments and identity virtualization at low cost to end users," in *IEEE Consumer Electronics Magazine*, vol. 6, no. 2, pp. 78-88, April 2017.
[16] Sung-Wook Park and Im-Yeong Lee, "Mutual Authentication Scheme Based on Lattice for NFC-PCM Payment Service Environment", *Sage Pub Journal*, 2016
[17] N. E. Madhoun, F. Guenane and G. Pujolle, *"A cloud-based secure authentication protocol for contactless-NFC payment,"* 2015 IEEE 4th International Conference on Cloud Networking (CloudNet), Niagara Falls, ON, 2015, pp. 328-330.
[18] Kai Fan, Panfei Song, and Yintang Yang, "ULMAP: Ultralightweight NFC Mutual Authentication Protocol with Pseudonyms in the Tag for IoT in 5G", *Hindawi Mobile Information Systems*, 2017
[19] Kai Fan, Panfei Song, Zhao Du, "NFC Secure Payment and Verification Scheme with CS E-Ticket", Hindawi, 2017
[20] R. Jin, X. Du, Z. Deng, K. Zeng and J. Xu, "Practical Secret Key Agreement for Full-Duplex Near Field Communications," in *IEEE Transactions on Mobile Computing*, vol. 15, no. 4, pp. 938-951, April 1 2016.
[21] Vanga Odelu, Ashok Kumar Das, and Adrijit Goswami, "SEAP: Secure and Efficient Authentication Protocol for NFC Applications Using Pseudonyms", IEEE *Transactions on Consumer Electronics*, Vol. 62, No. 1, February 2016.
[22] Busra Ozdenizci, Kerem Ok, and Vedat Coskun, "A Tokenization-Based Communication Architecture for HCE-Enabled NFC Services", *Hindawi Publishing Corporation Mobile Information Systems*, 2016.
[23] S. Rios, J.A. Morente and J. Pascual, "EXAMINapp: An Evolved Secure Anonymous Assessment Information System Using NFC And QR Technologies", *IEEE Latin America Transactions*, vol. 14, no. 6, June 2016.
[24] Mohamed Hamdy Eldefrawy and Muhammad Khurram Khan, "Banknote Validation through an Embedded RFID Chip and an NFC-Enabled Smartphone", *Hindawi Publishing Corporation Mathematical Problems in Engineering*, 2015.
[25] Debiao He, Neeraj Kumar, Jong-Hyouk Lee, "Secure Pseudonym-based Near Field Communication Protocol for the Consumer Internet of Things", *IEEE Transactions on Consumer Electronics*, Vol. 61, No. 1, February 2015.
[26] Rolando Trujillo-Rasua, Benjamin Martin, and Gildas Avoine, "Distance Bounding Facing Both Mafia and Distance Frauds", *IEEE Transactions on Wireless Communications*, vol. 13, no. 10, October 2014.
[27] K. Ren, Q. Wang, D. Ma and X. Jia, "Securing emerging short range wireless communications: the state of the art," in *IEEE Wireless Communications*, vol. 21, no. 6, pp. 153-159, December 2014.
[28] Tao-Ku Chang, "A Secure Operational Model for Mobile Payments", Hindawi Publishing Corporation, *Scientific World Journal*, 2014.
[29] Thomas Plos, Michael Hutter, Martin Feldhofer, "Security-Enabled Near-Field Communication Tag With Flexible Architecture Supporting Asymmetric Cryptography", *IEEE Transactions On Very Large Scale Integration (VLSI) Systems*, vol. 21, no. 11, November 2013.
[30] H. Eun, H. Lee and H. Oh, "Conditional privacy preserving security protocol for NFC applications," in *IEEE Transactions on Consumer Electronics*, vol. 59, no. 1, pp. 153-160, February 2013.
[31] Jeremy Gummeson, Bodhi Priyantha, Deepak Ganesan, "EnGarde: Protecting the Mobile Phone from Malicious NFC Interactions", ACM- MobiSys, 2013
[32] Rajalakshmi Nandakumar, Krishna Kant Chintalapudi, Venkata N. Padmanabhan, "Dhwani: Secure Peer-to-Peer Acoustic NFC", ACM-SIGGCOMM, 2013
[33] A. Matos, D. Romão and P. Trezentos, *"Secure hotspot authentication through a Near Field Communication side-channel,"* 2012 IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Barcelona, 2012, pp. 807-814.

BIOGRAPHIES OF AUTHORS

Ms. Anusha R. was born in Mangalore. She has received B.E. from NMAM Institute of Technology, Nitte in 2012 and M.Tech from Srinivas Institute of Technology, Valachil in 2014. In 2014, she joined Department of Electronics and Communication, Shreedevi Institute of Technology, Mangalore as Assistant Professor. Since 2015 she has been with Department of Electronics and Communication, NMAMIT Nitte as Assistant Professor. Her current research interest includes Cryptography, VLSI, and Embedded Systems. She is a Life Member of the Indian Society for Technical Education (ISTE).

Dr. Veena Devi Shastrimath V was born in Mysore. She has received B.E. from SJCE, University of Mysore in 1991, M.Tech from MIT, Manipal in 2002, and has received her PhD from Mangalore University in the field of Digital Image Processing and Remote sensing in May 2015. She is having teaching experience in various colleges including SJCE Mysore, BITS Pilani, India, Mangalore University, PACE Mangalore, SJEC Mangalore and NMAMIT, Nitte. At present she is working as a Professor in the department of ECE, NMAMIT, Nitte. She is having total 19 years of teaching experience & 2 years of Industrial experience. She is a Life Member of the Indian Society for Technical Education (ISTE), and IEEE.