ISSN : 2350-0743

www.ijramr.com

International Journal of Recent Advances in Multidisciplinary Research
Vol. 04, Issue 06, pp.2619-2624, June, 2017

REVIEW ARTICLE

THIRD PARTY BASED SECURITY MECHANISM IN NFC

***[1]Chandan Kumar and [2]Harneet Kour**

[1]Research Fellow, Department of CSE, CGC-College of Engineering, Landran, Mohali, Chandigarh, India
[2]Assistant Professor, Department of CSE, CGC-College of Engineering, Landran, Mohali, Chandigarh, India

ARTICLE INFO

Article History:
Received 21st March, 2017
Received in revised form
09th April, 2017
Accepted 14th May, 2017
Published online 30th June, 2017

Keywords:
NFC, Third Party, Security,
Short Range, Communication.

ABSTRACT

Near Field Communication (NFC) is a short range remote correspondence innovation, which works in the guideline of attractive acceptance. A little electric current is made by per user that thus makes an attractive field in the physical between the gadgets. A tag gets empowered from the field. NFC labels are fit for store information in it and are either perused just or rewriteable. Due to its protected nature used to store individual information, for example, plastic and Visa data, PINs and systems administration contacts. The correspondence run in NFC is constrained to inside 10 centimeters; this gives a substantial level of characteristic security. Despite the fact that to keep the lost or stolen gadgets from unapproved NFC exchanges, validation or authentication ought to be performed before every exchange. This work provides high level security in NFC so that data received by the receiver should be error free. In this work, performance analysis is done by using different parameters and shows that proposed mechanism is more secure than others.

INTRODUCTION

Near field communication (NFC) is an arrangement of principles for advanced cells and comparative gadgets to produce radio correspondence with each other by various means like by touching them with each other or by bringing them into closeness i.e. close to couple of centimeters. Expected applications and Present have contactless information trade, streamlined setup and exchanges, of more mind boggling interchanges, for example, Wi-Fi. Correspondence is additionally conceivable between a NFC gadget and an unpowered NFC chip, called a tag. In ISO 18092 points of interest of NFC detail can be discovered (Hasoo, 2013). NFC principle character is that it's a remote correspondence interface with a working separation constrained to around 10 cm. It could be worked in various modes. The modes are separated it is possible that it makes its own RF field or by recovering the power from a RF field created by another gadget. Dynamic gadgets are the gadgets which produce their own field if not, then is it known as latent gadget. Dynamic gadgets primarily have their own energy supply, though detached don't. Three unique setups are conceivable when two gadgets speak with each other. As of now, NFC innovation is dealt with additional as an information system for propelling different correspondences advancements than as a radio sort for real information move in focused utilize cases. While the NFC innovation bolsters augmentation systems for exchange of a lot of information, the present radio recurrence distribution to NFC requires closeness of NFC gadgets amid cooperations, which makes a client experience that is not helpful for long information exchanges. This is the reason NFC is ordinarily anticipated that would be utilized for either little information exchange connections or for propelling bigger information exchanges with an option portable remote correspondence innovation, for example, Bluetooth, WI-Fi, and versatile information benefit. Close field correspondence (NFC) is a ultra-short-run advancement that was planned for secure portion trades and similar applications. It most prominent range is around 20 cm, with 4 to 5 cm being a consistent association expel. This short partition fundamentally enhances the security of the affiliation, which is furthermore ordinarily mixed. Numerous PDAs fuse NFC, and various others are depended upon to get it unavoidably. The goal is to execute NFC portion structures where customers can tap a portion terminal with their PDA instead of using a MasterCard. NFC uses the 13.56-MHz ISM repeat. At this low repeat, the transmit and get circle accepting wires work basically as the basic and helper windings of a transformer, independently. The transmission is by the alluring field of the banner rather than the running with electric field, which is less predominant in the nearby field. NFC is moreover used to scrutinize names that are controlled up by the round of questioning of a NFC transmitted banner. The unpowered names change over the RF movement into dc that powers a processor and memory that can give information related to the application.

Corresponding author: Chandan Kumar
Research Fellow, Department of CSE, CGC-College of Engineering, Landran, Mohali, Chandigarh, India

Third Party Based Security Approaches

A put stock in untouchable is a substance which supports joint efforts between two social events who both trust the outcast;

the Third Party reviews all fundamental trade correspondences between the get-togethers, in light of the straightforwardness of making tricky propelled substance. In TTP models, the depending parties use this trust to secure their own particular coordinated efforts. TTPs are fundamental in any number of business trades and in cryptographic automated trades and furthermore cryptographic traditions; for example, a verification control (CA) would issue a propelled character presentation to one of the two social occasions in the accompanying case. The CA then transforms into the Trusted-Third-Party to that assertions issuance (Florian Michahelles, 2014). In like way trades that need a pariah recordation would similarly require an outcast storage facility organization or something like that.

This trusted outcast can add to security in dispersed systems, in a couple ways:

- The trusted pariah can add to secret properties, for example holding favored bits of knowledge for a customer, and showing those puzzles just to reasonable remote servers. The insider realities would be kept from diseases that may go with self-confident ventures.
- The trusted untouchable can moreover add to reliability properties, for example checking drawing closer and dynamic data. In particular, the trusted outcast embedded in a center A can check and guarantee the messages that A sends to another center point B. The trusted pariah can secure B against A's deficiency or malice, for example against A's contaminations.

Related Work

Hasoo Eun et. al. (Hasoo Eun, 2013), states that in the past couple of years, flexible terminals have been released joined with (close field correspondence) NFC. NFCs utilization run has been broadened with the blend of adroit devices with NFC. In electronic portion it is depended upon to supplant Visas. In this association, there is a need to address security issues for NFC electronic portion to be vitalized. The at present used NFC security standard requires as a piece of the key strategy handle at adjusted regard customers open key. The essentialness of the message is in the use of settled keys like – open key (of NFC). By amassing the related messages a profile can be made by an aggressor on customer's open key. With the help of profile made, we can exchange off the security and reveal the customers. Here they tell about methodologies for security protection depending upon pseudonyms cook these issues. Beside this for unexpected security {protocol data unit} PDU is described. Customer can tell other social occasion that in concordance with the tradition said in the paper it will bestow. The discussed system triumphs in limiting computation and cost upgrade by utilizing the vocations of traits of NFC.

F.W. Jesudas et. al. (2014) progresses a round plan of compact ward dependent upon open gages of EHR for the utilization on tablet PCs and PDAs utilizing android organize which utilizes NFC for planning data, finding diverse techniques for association of PC, in therapeutic field work forms. Dependent upon conspicuous confirmation of patient normally through NFC by methods for PDA, late eventual outcomes of ward round can be seen easily by specialists, and information as to incorporate/modify ought to be conceivable without choosing the patient physically from the once-over. With the help of EHR prime cases and arrangements specialists no longer need to oblige themselves to some particular record of ward round. Vinay Gautam et. al. (2013), states that security augmentation is required in NFC with addition in number of unapproved customers. In this paper [UBEP] 'customer lead based overhauled tradition' is proposed for security upliftment as to NFC contraptions. It tackles relationship of structure with the customer. This tradition has factors of four one of a kind sorts [time, edge and detachment, touch} direct of customer to find endorsement and validity of customers. Parts can be practically identical at the period of relationship of customer with structure. For customer affirmation UBEP utilizes check game plan of two phases. In the main stage which is called 'securing stage' - it stores and get coordinated effort of customer with NFC and for future references same information is used. In the affirmation arrange which is the second one examination of past and current circumstance of association of customer close by check of modernized stamp is done to confirm customer finally. Ali Alshehri et. al. (2013) gives a NFC security tenets to huge gatherings needs, formal examination of security, to check whether these guidelines meet their targets and essentials. Here formal systems are used to separate adaptable coupon rules which are NFC based [FDR/Casper]. Makers looked a fault against tradition then gave an answer which gives sustenance accuse formally. Florian Michahelles et. al. (2014), have depicted that RFID is attracting enormous eagerness as it quickly transforms into an extensively sent unavoidable development. Subjects included organization of data proprietorship in supply chains made through RFID, joining of RFID and sensors, security and insurance, NFC applications, RFID-based range identifying, and creating examination challenges. A. Alzahrani et. al. (Ali Alzahrani, 2013) shown a broad examination of the NFC advancement and its security essentials for human administrations applications. They furthermore displayed another portrayal of NFC structure strikes using a novel multi-dimensional portrayal. The proposed gathering considers three essential perspectives to organize ambushes on NFC systems for restorative administrations applications. These perspectives are: technique for operation, programmability level, and life cycle. Using the proposed plan, the possible risks to NFC structures in human administrations applications and discuss possible vulnerabilities and challenges related to NFC security in the social protection field are examined.

Proposed Work

The improvement of new progressions get ready to the development of new devices that sporadically ought to be interconnected with a particular true objective to get to or share available resources or organizations among them. Different particular remote advances have been made for short partitions. These are insinuated as 'short-range remote correspondence. Signals go from two or three centimeters to a couple meters. The short range correspondence structures give remote accessibility inside a close-by hover of correspondence. The confined extent of remote correspondence can offer a security highlights. Close Field Communication (NFC) is a short range remote correspondence development, which works in the rule of appealing acknowledgment. Somewhat electric current is made by per client that subsequently makes an appealing field

in the physical between the devices. A tag gets engaged from the field. NFC marks are fit for store data in it and are either examined just or rewriteable. Because of its ensured nature used to store singular data, for instance, plastic and Visa information, PINs and frameworks organization contacts. The correspondence keep running in NFC is obliged to inside 10 centimeters; this gives a significant level of trademark security. In spite of the way that to keep the lost or stolen contraptions from unapproved NFC trades, approval or validation should be performed before each trade. This work is gives abnormal state security in NFC with the goal that information got by the collector ought to be sans mistake. This proposed work is to give validation based security utilizing Third gathering approach where outsider appoint keys to the whole system and data exchanged to just the verification hubs. This improves the security level in NFC and abatements loss of information. The fundamental plan of the proposed work is as given in Fig 1.

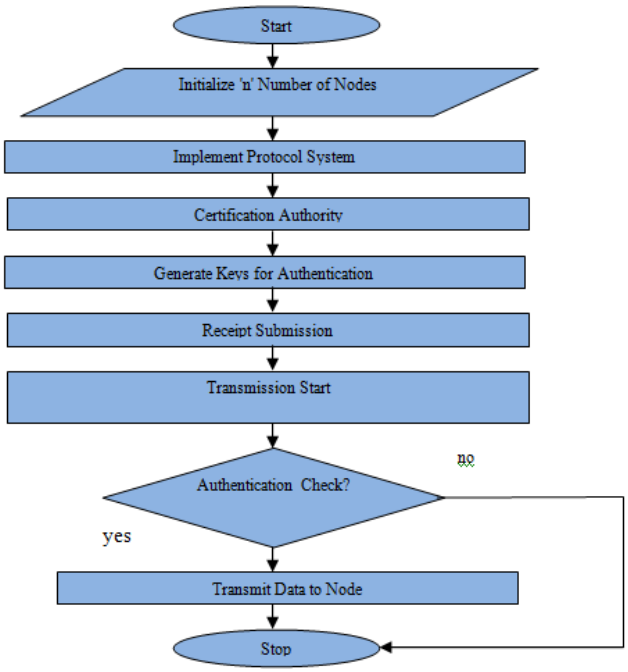

Fig. 1. Proposed Methodology

Simulation Parameters

The simulation has been performed using NS-2.35. Simulation has been performed by taking the simulation parameters as stated in Table 1. The trace files have been generated by simulating the scenario and with the help of XGRAPH and AWK files results are formulated.

Table 1. Simulation Setup

Parameter	Value
Channel Type	Channel/WirelessChannel
Radio-propagation model	Propagation/TwoRayGround
Network interface type	Phy/WirelessPhy
MAC type	Mac/802_11
Interface queue type	CMUPriQueue
Link layer type	LL
Antenna model	Antenna/OmniAntenna
Max packet in ifq	500
Number of nodes	35
Protocol	NFCIP
X axis distance	1600
Y axis distance	1050

Step wise Explanation

Step 1- Generate Network Scenario

The first step of the simulation is to generate network scenario. In this scenario 35 nodes are generated in the area of 1600x1050. In this, one node is treated as third party and one is as base station of the network.

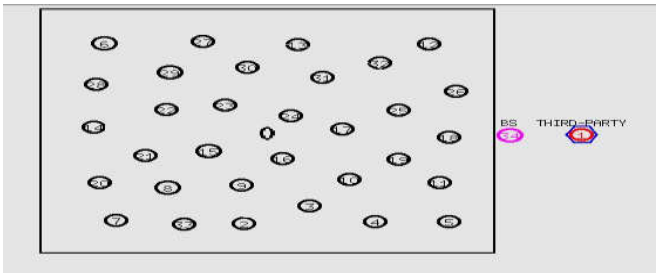

Fig. 2. Network Scenario

Step 2: Key Generation and Distribution

In this work, a third party is used for security purposes. Third party generates authentication keys and distributes it to all other nodes in the network through base station. These keys will be used for authentication purposes when communication between the nodes will take place.

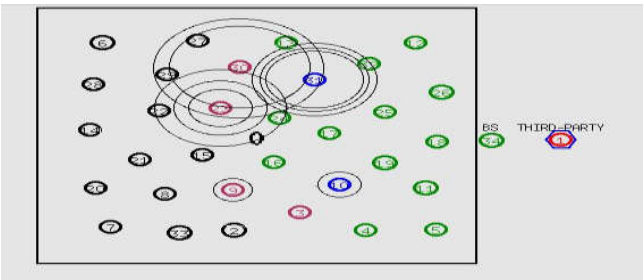

Fig. 3. Key Generation and Distribution

Step 3: Receipt Submission

After receiving authentication keys, nodes will send receipt or acknowledgement to the third party that key has been received. So that authenticated nodes are verified by the third party.

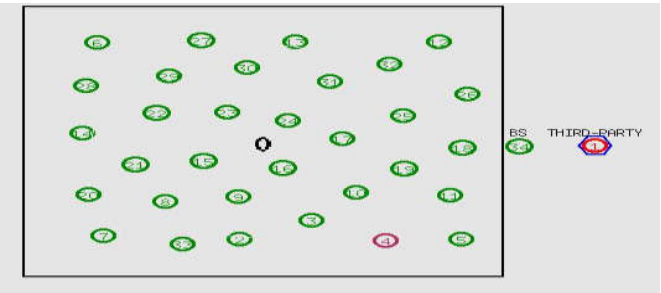

Fig. 4. Receipt Submission to Third Party

Step 4: Source and Destination

In this scenario, user will enter source and destination node address it means nodes are selected which you want to connect for data sharing. In this work, source node firstly send the

request message for establish connection between two nodes. Both nodes establish connection only if they were authenticated nodes of the network.

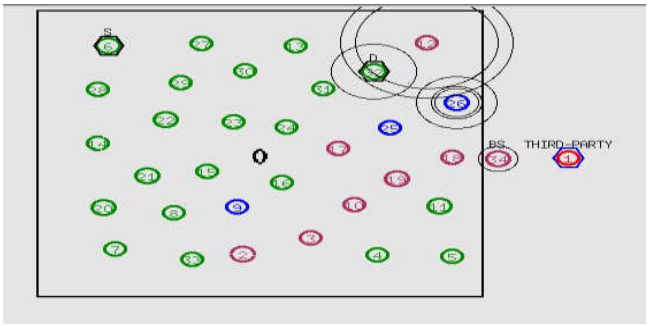

Fig. 5. Source and Destination

Step 5: Route Reply

Once the request is received by the destination, destination waits till default waiting time and then send route reply through the authenticated nodes of the network.

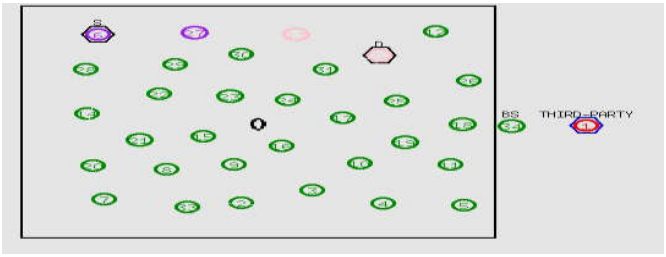

Fig. 6. Route Reply

Step 6: Data Transmission

When source node receives reply packet then it will send its data packet. The data packets also encrypted before transmitting at the source side. Destination decrypts these data packets using the same symmetric key.

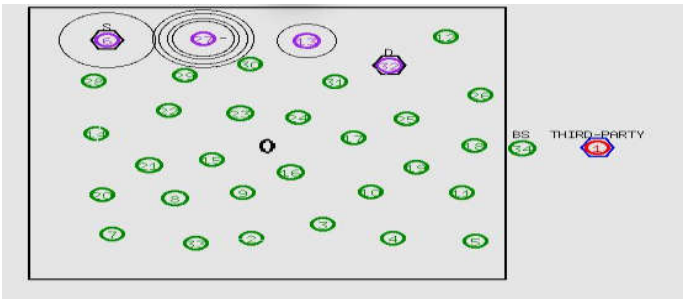

Fig. 7. Data Transmission

Performance Analysis

This proposed work is to enhance the Security in NFC where a third party based Security mechanism is proposed. So, to analyze the performance of the proposed mechanism following performance metrics are considered.

- Average End to End Delay
- Average Energy
- Throughput
- Packet Delivery Ratio
- Key Size
- Key Generation Time

Average End to End Delay: This includes all possible delays caused by buffering during route discovery, latency, and retransmission by intermediate nodes, processing delay and propagation delay. It is calculated as

$$D_i = (Tr - Ts)$$

Where, T_r is receive time and T_s is sent time of the packet. Where average delay is computed as:

$$Avg_{Delay} = \frac{1}{n}\sum_{i=1}^{n} D_i$$

Table 1 gives the Average Delay values for both Previous and Proposed Mechanism.

Table 2. Average Delay in ms

Sr. No.	Time	Existing	Proposed
1	5	0	0
2	10	21	0.01
3	15	53	0.01
4	20	53	0.01
5	25	33	0.01

Table shows that proposed mechanism reduces average delay as compare to existing mechanism. Table shows that on an average this proposed mechanism improves 99% performance by reducing delay near to null.

Average Energy: In this, Average Energy is taken as a residual energy which is the amount of energy left after transmission starts. It is calculated as:

$$Avg_{Energy} = T_E - (E_S + E_R)$$

Where, T_E is the Total Energy and E_S & E_R is the energy consumed during sending and receiving packets throughout the transmission. Table 2 gives the Average Energy values for both Previous and Proposed Mechanism.

Tabel 3. Avg. Energy in Joules

Sr. No.	Time	Existing	Proposed
1	5	97.38	99.43
2	10	93.8	96.24
3	15	89.17	95.29
4	20	81.74	93.64

Table shows that proposed mechanism increases the average energy as compare to existing mechanism. Table shows that on an average this proposed mechanism improves 6% performance by reducing energy consumption and improving Average Energy.

Throughput: It is the average at which data packet is delivered successfully from one node to another over a communication network. It is usually measured in bits per second.

$T\square roug\square put = (no\ of\ delivered\ packets * packet\ size)/ total\ duration\ of\ simulation$

Table 4 gives the Throughput values for both Previous and Proposed Mechanism

Tabel 4. Throughput in kbps

Sr. No.	Time	Existing	Proposed
1	5	2.32	2.32
2	10	5.43	5.43
3	15	40.2	80.37
4	20	99.28	165.76
5	25	131.67	178.48

Table shows that proposed mechanism increases the Throughput as compare to existing mechanism. Table shows that on an average this proposed mechanism improves 23% performance by increases Throughput.

Packet Delivery Ratio (PDR): It is defined as the ratio of data packets actually received at the receiver end to those which were sent by sender. So, it can also be defined as:

$$PDR = {}^{R_i}/_{S_i}$$

Where S_i is the total number of data packets sent by the nodes in the network and whereas R_i is the total number of data packets received by the receivers.

Table 5. Gives the PDR values for both Previous and Proposed Mechanism

Tabel 5. PDR in prcentage

Sr. No.	Time	Existing	Proposed
1	5	48.13%	48.13%
2	10	99.43%	99.43%
3	15	99.87%	96.45%
4	20	99.87%	99.87%
5	25	99.87%	99.87%

Table shows that proposed mechanism increases the PDR as compare to existing mechanism. Table shows that on an average this proposed mechanism improves 0.6% performance by increases PDR.

Key Size: *Key size* or *key* length is the number of bits in a *key* used. Key Size needs to be less so that it will reduce the extra requirement of energy and time. This proposed mechanism also helps to reduce the key size as compare to the existing as shown in Fig 8.

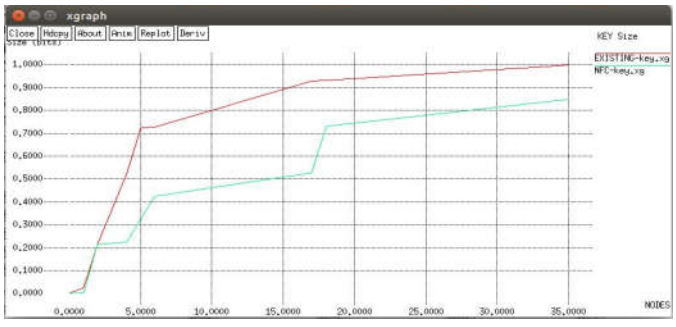

Fig. 8. Key Size

Key Generation Time: *It is defined as a time taken by the mechanism to generate keys for authentication*. This proposed mechanism also helps to reduce the key generation time as compare to the existing as shown in fig 9.

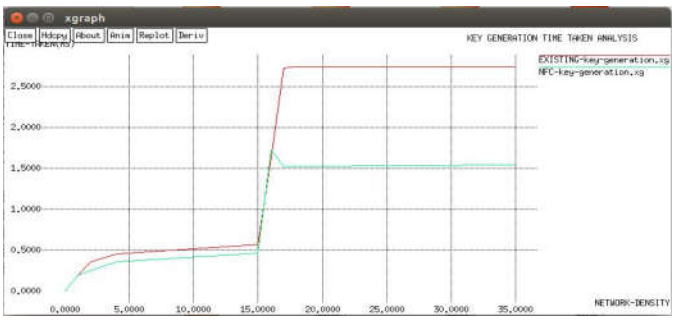

Fig. 9. Key Generation Time

Conclusion

With late arrival of different terminals outfitted with NFC (Near Field Communication), e-installment showcase utilizing NFC is relied upon to be enacted. In such circumstance, the client's exchange data holes can prompt to the attack of security. Condition protection safeguarding convention is a technique for secure correspondence with NFC structure with various pen name strategy and give contingent PDU to further security of individual correspondence of client. Giving nom de plumes fundamental to keep up secure recognizable proof of the client and are extremely valuable in staying away from man in center assault. Various pen names by Trusted Service Manager is huge favorable position yet needs in putting away, preparing and correspondence cost. In the proposed framework another system, that is Third gathering based confirmation, is utilized for decreasing information misfortune and to give abnormal state security. In this technique, arrange condition is produced and afterward proposed strategy is executed. The technique lessens the key stockpiling prerequisite and additionally Delay and enhances the Packet Delivery Ratio, and throughput is expanded on the created arrange. The proposed techniques take after standard frameworks and conventions. In conclusion it is normal that the proposed framework will decrease the capacity prerequisites and to upgrade other execution networks. It will add to advancement of NFC applications in cell phones. Future work go in course to test and examination the execution of this upgraded framework by actualizing in various NFC applications and furthermore test the framework with other security strategies to enhance their productivity and security.

REFERENCES

Ali Alshehri, Johann A. Briffa, Steve Schneider and Stephan Wesemeyer" Formal Security Analysis of NFC M-coupon Protocols using Casper/FDR". IEEE workshop on NFC Communication 2013

Ali Alzahrani, Abdullah Alqhtani, Haytham Elmiligi, Fayez Gebali, Mohamed S. Yasein. "NFC security analysis and vulnerabilities in healthcare applications," IEEE Pacific Rim Conference on Computers and Signal Processing (PACRIM), 2013.

Antonio J, Alcolea, Alberto F. ; Zamora, Miguel A. ; Skarmeta, Antonio F, "Evaluation of the security capabilities on NFC-

powered devices", IEEE Workshop on Smart Objects: Systems, Technologies and Applications (RFID Sys Tech), June 2010.

Arnau Vives-Guasch, Magdalena Payeras, Macia M.Puigserver, Jordi Castell,"Secure e-ticketing scheme for mobile devices with Near Field

Briffa, Johann A., "Formal security analysis of NFC M-coupon protocols using Casper/FDR", IEEE Workshop on Near Field Communication (NFC) , pp1 – 6, Feb. 2013.

Communication (NFC) that includes exculpability and reusability", IEICE Transactions Fundamentals, Vol.E93–A, No.1 January 2010.

Dirar Abu-Saymeh, Dhiah El Diehn I. Abou-Tair, Ahmad Zmily, "An Application Security Framework for Near Field Communication", 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), July 2013

Eric Krevice Prebys," The Genetic Algorithm in Computer Science", MIT Undergraduate Journal of Mathematics,2002.

Florian Michahelles, Frederic Thiesse, Albrecht Schmidt, John R. Williams "Pervasive RFID and Near Field Communication Technology", IEEE Computer Society, Vol.33, No.1, pp.34-39, Jan 2014.

G.Gopichand, T.Krishna Chaitanya , R.Ravi Kumar" Near Field Communication and Its Applications in Various Fields "International Journal of Engineering Trends and Technology (IJETT) ,Volume 4, Issue 4, April 2013

Hancke, G, Markus G. Kuhn "A Security Framework Model with Communication Protocol Translator Interface for Enhancing NFC Transactions ", IEEE Conference on Advanced Telecommunications(AICT) pp 452-461 May 2010

Hasoo Eun, Hoonjung Lee and Heekuck Oh "Conditional Privacy Preserving Security Protocol for NFC Applications", IEEE Transactions on Consumer Electronics, Vol.59, No.1,pp.128-134, February 2013.

Hussein Ahmad AL-Ofeishat, Mohammad A.A.AL Rababah," Near Field Communication (NFC)", International Journal of Computer Science and Network Security, VOL.12 No.2, February 2012

Jeffrey Fischer,"NFC inCell Phones: The New Paradigm for an Interactive World", Foundations and Trends in IEEE Communications Magazine, No.1–2, June, 2009.

Jesudas, F.W., V.Gowri, M.Sherwin Nayanar, "Conditional Privacy Preserving Security Protocol for NFC Application" IJCSMC, Vol. 3, Issue. 2, February 2014

K.Preethi, Anjali Sinha ,Nandini" Contactless Communication through Near Field Communication" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012

L Francis, G Hancke, K Mayes, K Markantonakis "Potential misuse of NFC enabled mobile phones with embedded security elements as contactless attack platforms", IEEE Conference for Internet Technology and Secured Transactions,(ICITST) , pp 1 – 8, 2009

Madlmayr, G, J. Scharinger " NFC Devices: Security and Privacy", IEEE International Conference on Availaibility, Reliability and Security,ARES 08 pp 642 – 647, 2008

Roy Want," Near Field Communication", IEEE Communications Magazine, Vol.16, No.9, pp.28-29, September 2011.

Vedat Coskun, Busra Ozdenizci, Kerem Ok,"A Survey on Near Field Communication (NFC) Technology", Springer journal on Wireless Personal Communications, Volume 71, Issue 3, pp 2259-2294, August 2013

Vinay Gautam, Vivek Gautam" User Behavior Based Enhanced Protocol (UBEP) for Secure Near Field Communication", *International Journal of Computer Applications* Vol:7 No:11, 2013.

****