*Impact Factor (SJIF): 3.632*

**International Journal of Advance Research in Engineering, Science & Technology**

*e-ISSN: 2393-9877, p-ISSN: 2394-2444*

***Volume 3, Issue 10, October-2016***

# HOW TO MORE SECURE IN ONLINE TRANSACTION USING NEAR FIELD COMMUNICATION

KEDARE AJAY PANDITRAO

*MCA DEPARTMENT JNEC AURANGABAD(M.S)*

***Abstract —This paper analysis provide how to more secure of data using nfc. Nfc techonology can be used today to day activity more secure.like nfc used in shopping mall.nfc used in smart fitness.smart secure of data using nfc.smart payment payment can be done easily using nfc.nfc tag usedfor security at organization level.***

***Keywords-nfc tag nfc devices retinascanner. ; style; styling; insert (key words) (minimum 5 keyword require) [10pt, Times new roman,Italic, line spacing 1.0]***

## I. INTRODUCTION

NFC technology is a standard based wireless technology that allow data to be exchange between devices that are a few centimeters apart. NFC operates at 13.56 mhz and transfer data at upto 424kbites/second.NFC is distinguished by it intuitive interface and its ability enable networking platform . Access digital content using wireless such as mobile phone enabled RF tag.

Making payment with a wave or touch anyware contactless card point of sale. Storing tickets . Today the rapid development and adoption of information technologies is changing the way of doing business significantly. The growing interest on electronic commerce to perform business transactions brought vital improvements, especially in contactless technologies [1]. Near Field Communication (NFC) has become one of the promising technological developments in IT industry. NFC technology is a short-range, high frequency, low bandwidth and wireless communication technology based on Radio Frequency Identification (RFID) technology. It allows us to transfer data within few centimeters. One of the advantages of NFC over other wireless technologies is simplicity (Madlmayret al. 2008): transactions are initialized automatically after touching a reader, another NFC device or an NFC compliant transponder. Due to its simplicity, it has become a new and exciting area for practitioners, many NFC enabled applications and services are developed which are operating in three different modes; reader/writer, peer-to-peer and card emulation [2]. The integration of NFC technology into mobile devices offers many reliable applications; specifically payment, ticketing, loyalty services, identification, access control, content distribution, smart advertising, peer-to-peer data/money transfers, and set-up servicesWith NFCtechnology, communication is established when an NFC-compatible device is brought within a few centimetres of another i.e. around 20 cm theoretically (4cm is practical). The immense benefit of the shorttransmission range is that it prevents eavesdropping on NFC-enabled dealings. NFC technology enablesseveral innovative usage scenarios for mobile devices. NFC technology works on the basis of RFIDtechnology which uses magnetic field induction to commence communication between electronic devices inclose vicinity. NFC operates at 13.56MHz and has 424kbps maximum data transfer rate. NFC iscomplementary to Bluetooth and 802.11 with their long distance capabilities. In card emulation mode NFCdevices can offer contactless/wireless smart card standard. This technology enables smart phones toreplace traditional plastic cards for the purpose of ticketing, payment, etc. Sharing (share files betweenphones), service discovery i.e. get information by touching smart phones etc. are other possibleapplications of NFC using smart phones. This paper provides an overview of NFC technology in a detailedmanner including working principle, transmission details, protocols and standards, application scenarios,future market, security standards and vendor's chipsets which are available for this standard. Thiscomprehensive survey should serve as a useful guide for students, researchers and academicians who areinterested in NFC Technology and its applications. Nowadays the increasing mobility of devices provided by mobile communications has become animportant feature in the emerging technical world. Before the introduction of Near FieldCommunication (NFC) technology, the mobile phones already had several types ofcommunication options with the external environment .When the mobile phones were introduced, the primary need was to setup voice communication, it was primarily provided by Global Systemfor Mobiles (GSM) which has other services such as SMS, MMS and even internet access. LaterBluetooth technology was introduced that connects peripherals with computing devices includingmobile phones [1]In present days, a new communication technology known as NFC is becoming popular in mobilesmart phones. This technology needs two NFC compatible devices placed very near to each other(less than 4cm) in order to communicate. In an NFC communication, twodevices are needed. First device is called the initiator which is an active device and is responsiblefor starting the communication, whereas second device is called the target and responds to theinitiator's requests. The target device may be active or passive. The communication starts whenthe active device gets close to the target and generates a 13.56 MHz magnetic field and powersthe target device [3] (See Figure 1).The NFC technology works via magnetic field inductionand operates on an unlicensed radio frequency band. Also it includes an embedded energy sourcecomponent whereas thetarget can be a RFID card, tag or an NFC device which gives the reply toinitiator's request .

NFC uses an inductive coupling technique comparable to the transformer principle i.e. the magnetic near-field of two conductor coils is used to pair the initiator (Polling) device and target (Listener) device (See Figure 1)[1]. In this pairing of the coils of initiator and target, a passive listening device also affects the active polling device. A variation in the impedance of the listening device results in an amplitude or phase changes to the antenna voltage of the polling device, detected by the polling device [2].
How to actual transmit information on NFC

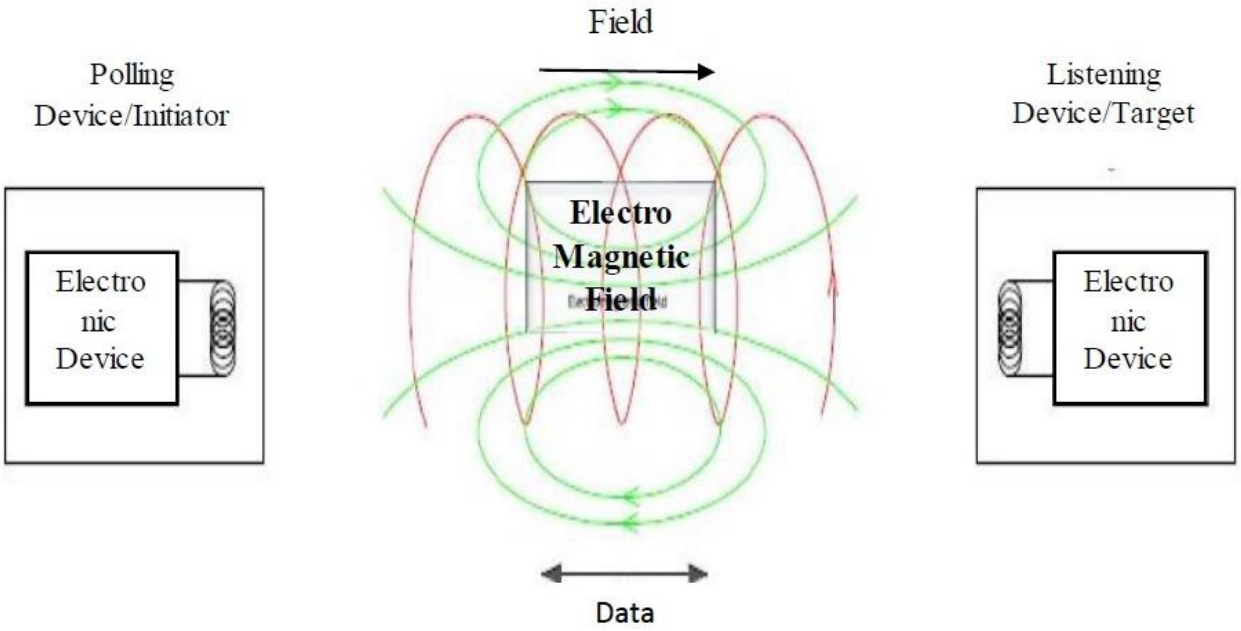
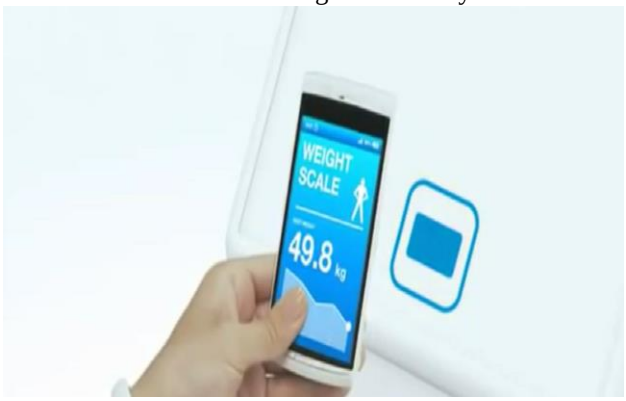



Figure 1: NFC Transmission[1]

**NFC OPERATION MODES**
1)Reader/Writer mode
2) card emulation mode,
**3)** Peer to peer mode
1)Reader/Writer mode of operation the application transfers data in NFC forum defined messageformat. In this mode the NFC enabled mobile phone can perform read/write operation on NFCtags. In Reader Mode, NFC initiator reads data from the NFC tag where as in the writer mode,initiator writes data in to the tag. It should be noted that Reader/Writer mode of communication isnot secure. The applications supported by this mode are,Smart Poster Remote Marketing Remote Shopping Social Networking Location based services.
2) card emulation mode, the NFC enabled mobile device acts as a contactless smart card. Theexamples of smart card are debit card, credit card, access cards etc. Data transfer in this mode ishighly secure. This mode supports the following applications.Payment Loyalty Ticketing Access control Identity Services.
3) Peer to peer mode supports link level communication. It supports two NFC enabled device toexchange information such as a text message, contact record or data of any other kind. NFCIP-1and LLCP are the two standardized options in peer to peer mode. This mode of communication issecure. The applications supported by this mode are the following.
Exchanging Data Money Transfer Social Networking.

NFC can be used for
a) Smart Entertainment
b) Smart Work: One can use different NFC Tags to make work easier and smart.
c)Smart Fitness: Using NFC one can get the status his fitness.
d) Smart Payment: Payment can be done easily using NFC.
E) Smart Security: NFC Tags can be used for security at organizational level.

We have introduced following inovative system better than existing system




Smart Fitness

Smart security


Smart Payment

How To Secure NFC Transactions

Security threats in current uses of NFC are well understood from similar applications in areas like content distribution (DRM), web browsing, and networking. Here we discuss techniques and principles to provide security in NFC-based applications.

Preventing unauthorized ticket sharing

In the case of electronically presented service "tickets", such as in public transportation or sports events without assigned seating, we have to ensure that users can not share their benefits with other parties. Consider the case of Shawn who has a ticket to watch the San Jose Sharks. Shawn decides to share his ticket with a friend: he beams the contents of theticket over to Sara's smartphone, and now both of them can present a valid token at the entrance.

The means of dealing with unauthorized sharing dependheavily on the level of protection desired. At one end of the spectrum, a centralized database can keep track of used ticketsat the venue, and a ticket becomes invalid once presented.Either Shawn or Sara can get in, but not both of them. Optionally,the ticket can be made valid again in case the ownerexits the venue, to allow re-entry. Note that if transfer of ownership must be supported, then centralized tracking ofownership has to be in place from the time of ticket issue, all the way to the time of use.A less centralized solution involves tickets that are tied to a specific person: at the time of ticket generation, the issuing authority uses a private key to sign the ticket along with a photo of the authorized owner. The benefits of this approach extend to long-term tickets that can be used multiple times(such as commuter rail permits or ski passes). Finally, in situations where long-term permits are not visually checked(such as in high-traffic areas like the subway), data mining can be used to verify legitimate use and flag suspicious cases for examination or even revocation.

Securing Contextual Application Invocation

The smart phone reading passive content over NFC will be a dominant mode of interaction. Several security principles underpin such operations both for the purpose of contextual application invocation. These principles derive from the analogy to browsing on the Internet and following links: we learn to be careful when navigating to unknown domains, and modern browsers offer much assistance in helping us make the correct decisions. The content scanned must be assumed insecure and should not be trusted in any critical or expensive actions. Specifically ,data received over NFC should not lead to arbitrary behind-the-scenes activities, such as sending SMS or performing a phone call [1]. Rather,

every scan should either lead to no "side effects", or such effects have to be explicitly described to the user prior to taking the action to give her an opportunity to verify the action taken (e.g. confirm the outgoing call or SMS, or verify that the domain being browsed is correct before navigating to it [2]). This of course extends to loading and running applications which require any privileges
(access to private data, Internet access, and so on). Although visual cues can be provided to a user that the scanned tag has not been tampered with, ultimately trust in the content must start with a signature from a known entity

Man-in-the-Middle Attacks
With NFC, we must watch out for the possibility for an attacker, a third party with an active tag, to inject itself in the conversation and modify it to his advantage possibly even without being noticed. While peer certificates can go a long way towards excluding third parties from an exchange, they will never be the complete answer: certificates can be obtain edfraudulently, or perhaps with an apparent owner which appears to be legitimate, but is not (such as using a slightly misspelled version of the legitimate owner). Because of this ,it is imperative that interactions be designed with multiple safeguards: verification based on cryptography, as well as user verification and common sense (e.g. when confirming a payment ,there should not be two or more simultaneous payment requests from different payees, Figure 2[2]; or, when payment is confirmed but the service is still unavailable, assume fraudulent use—the payment went to the wrong destination—so the user should investigate).

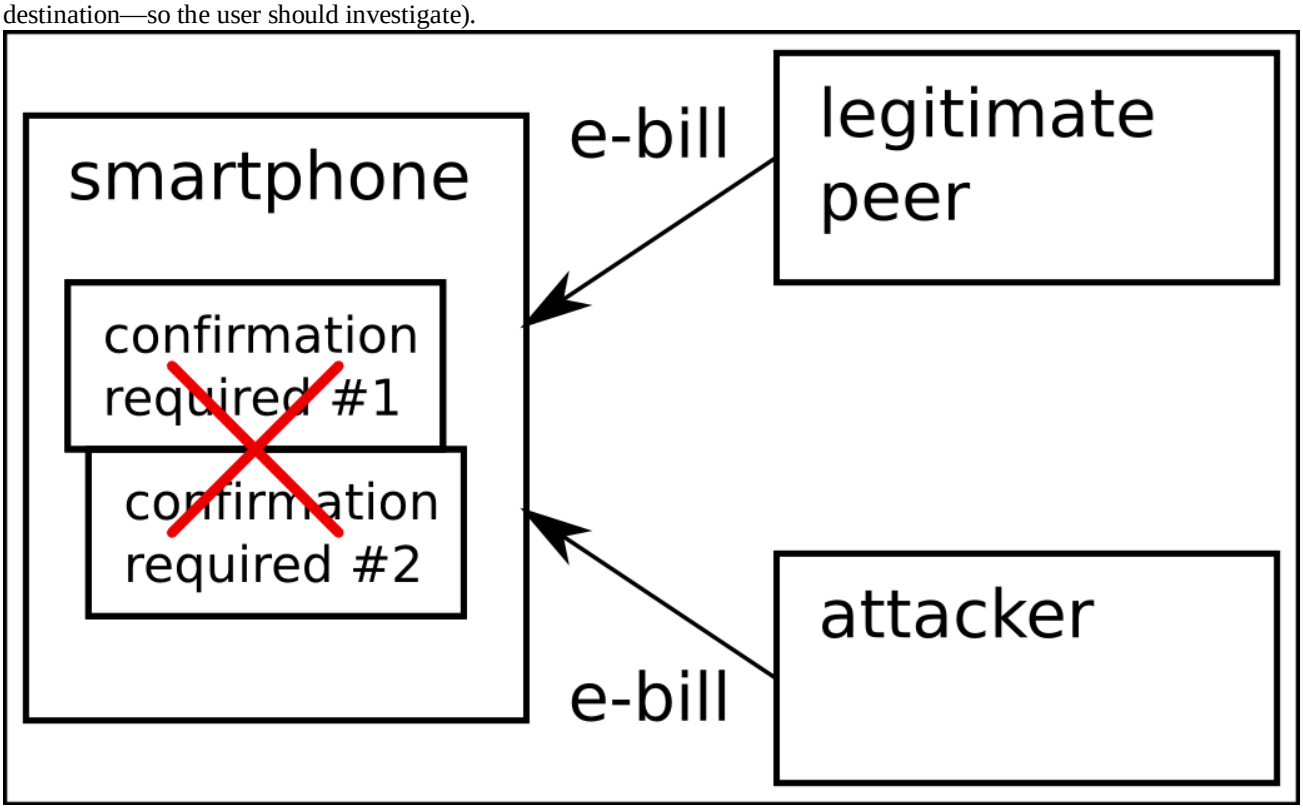



Figure 2: Security-aware interaction design[2].
Two simultaneous ebills (a very rare occurrence) are flagged and assumed malicious by the payment application

Preventing relay attacks In a relay attack the authentication protocol is bridged, such that authentication no longer requires physical proximity [1]. Users transacting unique low-cost objects (such as people presenting movie tickets at the entrance) are particularly vulnerable to relay attacks. On the one hand, the low value of the transaction makes an interaction-free approach more acceptable. On the other hand, if the object owner is willing to publicly share the object, then she becomes vulnerable to malicious relaying of the ticket and involuntarily granting entry to an attacker. While relay attacks can be prevented by distance bounding [3], the technology is still in its infancy :a simpler approach could be to give ticket owners a choice between security (user confirmation required to use the ticket)and convenience (the ticket is presented automatically). This behavior could adjust based on context: the ticket management .application can decide whether it is safe to present a token without asking the user—based on the device location and past history of fraud at that location.

**REFERENCES**

1)Ernst Haselsteiner and Klemens Breitfuß"Security in Near Field Communication (NFC)"

2)K.Preethi , Anjali Sinha ,Nandini."Contactless Communication through Near Field Communication".

3)Hussein ahmad Al-Ofeishat,Mohammad A.A.AL.Rababah."near field communication.