



A Literature Survey on Near Field Communication (NFC)

Tarang, Rhythm, Tamalika
School of Computer Science and Engineering
VIT University, Vellore-14, Tamil Nadu, India

Abstract: We here are presenting the idea of NFC. We have analysed around 35 research papers for formulating one final document which explains the NFC and all its components along with advantages and disadvantages it possesses. NFC is the short form of Near Field Communication which can be considered to be the higher extension of Wireless communication in the modern day world. Why should we use NFC? The answer to this question is faster data transfer rate compared to other wireless options available. The main issue that might occur though is the security of NFC. The paper also presents the scope of NFC in the near future. This paper proposes the various fields where NFC technology can be used. The most useful application is the online bill payment through your mobile. Also NFC can be used widely in the medical sector providing much more accurate results and better diagnosis. This paper thus presents the probable use of NFC in various fields and its advantages.

Keywords: NFC, near field communication, smart phones, tags, transactions, wireless, connectionless technology, protocol, half duplex, full duplex, touch and run, range

I. INTRODUCTION

NFC is estimated as Near Field Communication which was introduced in 2002 by both Sony and Philips. It allows any two devices which have NFC in them to communicate with each other when the two devices are in close proximity of about 4 cm. The main advantage of using NFC is that no communication links have to be established first due to which it is faster than the existing technologies. NFC uses two types of encoding techniques for the process of exchanging data. These two techniques are Miller Coding and Manchester Coding. Miller coding has 100 percent modulation whereas Manchester Coding has modulation ratio of 10 percent. When the baud rate is 106KB then Miller Coding has been used and in every other case Manchester Coding has been used. NFC can be used in many applications because it allows both one way and two-way communication. NFC is based completely on RFID. Each NFC device can operate in three distinctively unique modes. NFC is compatible to legacy contactless smartcard systems based on the standards ISO/IEC and Felicia. Beside that standardisation through bodies such as ISO/IEC and ECMA various data forms, normalised data's, basic requirements, device certification. The fundamental property by which NFC works is- 'it is all in one touch'. This means that just one touch or contact between two NFC enabled devices triggers an action in both of them. objects are embedded with NFC tags which store content like internet access address(URLs), phone numbers, SMSs and business cards. NFC works in three basic modes namely-peer-to-peer mode, reader/writer mode and card emulation modes. One of the prime reasons that a lot of research work is being carried out in the field of NFC is that our lives are more or less dependent on mobile phones and the concept of NFC is incorporated in mobile phones or smartphones. All the research carried out in this field points towards the various advantages which include faster transactions which are more reliable if certain parameters are kept in mind. The concept of NFC is still in the developing stage and has applications various different areas including Health Care, Payment, Business Transactions and in home security systems which can be extended further to regulate air conditioners and heaters. There are many loop holes and almost none of its present applications are full proof. The major areas of concern covered in this paper include attacks from a third party to either modify the data so that the receiver receives wrong data or to manipulate the data so that the receiver cannot understand what the sender wants to send, another theoretical but not practical issue is the Man-in-the-Middle-Attack. Further issues of compatibility with iPhone and interface problems have been highlighted along with new ideas to overcome these problems as suggested by the researchers. Newer applications have been developed and steps have been taken by companies like Google and Pay-Pal for the growth of this application. Further as compared by many other wireless technologies it is most easily adoptable mode for data transfer. NFC is basically a communication protocol used for wireless communication based on half duplex protocol. The communicating devices, one is known as the initiator which provides a path for the data to be transferred and the other device is known as the target which accepts the data or the requests which are been made by the initiator. The most secure part in a smart card microchip is that it has the capability to produce secure card emulation. Portable devices with NFC in it can be provided with applications which can read E-tags and make payments with an NFC enabled device. Earlier 'proximity card' technologies were used but NFC uses

electromagnetic induction between the two devices in loops which is operated within unlicensed radio frequency bandwidths. NFC tags are passive storage of data units which can be read and written too or by an NFC device. These tags can be encoded by their producers to use certain industry specifications and these specifications are provided by NFC FORUM. Secure communications in NFC are made available by applying cryptographic algorithms. NFC is completely based on RFID (Radio Frequency Identification). This technology is mostly used for identifying, authenticating and tracking information. The research related to this topic is being carried out from as late as 1983. Charles Walton started this research. The research gained its momentum in 2009 when a new NFC forum released peer-to-peer standards to ensure transferring of contacts, URLs, Bluetooth, etc. In 2010 Samsung launched its first android NFC phone – nexus. NFC is designed for short range wireless technologies. And its range is as less as 10 cm. There are 2 modes how NFC works namely active and passive. In the active mode, both the initiator and target communicate by alternately generating their own fields. The device deactivates its RF field. Both the devices typically have power supplies. In passive mode, the initiator provides a carrier field and target answers by modulating the existing field. The strong RF signals are transmitted through antennas. NFC standards cover communication protocols and are based on RFID standards. On November 17 2010, 3 companies launched a joint initiative to build a platform to make payment using NFC. It was initially known as mobile wallet. Also later it was called ‘soft card’. The venture which was designed in broad deployment of NFC technologies. On September 9 2014, Apple announced a new support for NFC power transactions which was included in the apple pay. Apple then claimed that their approach to NFC payment was better and secure. NFC can be used for social networking or sharing various contacts between 2 smartphones with NFC in it. Such devices can act as electronic identity and also key cards. The android smartphones can take advantage of their compatibility of working with various NFC application. Some of the common and popular are TagInfo, TagWriter by NXP, WifiTap Wi-Fi NFC, NFC Task Launcher, NFC classic tag reader writer. The current interest of researches is the advantages of NFC over Bluetooth and vice versa. Bluetooth and NFC share many features, like being forms of short distance wireless communication devices but where NFC can reach to a distance of 10 cm, Bluetooth extends to 30 feet. NFC consumes very little power in comparison to the Bluetooth technology. While NFC has to power a passive and unpowered source like an NFC tag it demands more power than a Bluetooth device, only in that situation. Another advantage of NFC is it is easy to use. Bluetooth demands users to first manually set up the connections between devices and takes some time. NFC gets connected automatically in a very little time. Although the users have to be close to each other for NFC usage, it is much faster and handier to set up than a Bluetooth connection. However recent developments in Bluetooth technology, Bluetooth low energy (BLE), aim at low power even lesser than NFC. As the technology advances, Bluetooth and NFC technology may work shoulder to shoulder, relying on each other to help different users to meet their data transmission requirements and fulfil them. There are several security issues in NFC one of them being the man-in-the-middle attack. With all of the above mentioned advantages, improvements and varieties of NFC’s applications all over the technological platform, it has its users increasing in a very alarming rate. We have chosen the topic henceforth. The apple iPhone 6 is the first apple phone which is compatible with NFC and around 40 devices have been launched in android which are compatible with this new technology. The Bluetooth headphones and speakers also can be a very good example of implementation of NFC.

II. ORGANIZATION

- Abstract: A brief idea of the research paper
- Keywords: Some of the important words that have been repeatedly used in the paper.
- Introduction: Explaining the basic model of the research topic.
- Organisation: Contents of the paper in a brief manner.
- Literature Survey: Providing the detail components of the research.
- Conclusion: The final conclusion of the research carried and its scope.
- References: The research papers referred for carrying out the research.

III. LITERATURE SURVEY

In the work carried out by Ernst Haselsteiner and Klemens Breitfub, the main aim was to point out the security issues related to NFC (Near Field Communication). Some practical solutions to these problems are also proposed in the research carried out by them. The communicating devices can be either active or passive. A communicating device is said to be active, if it generates its own RF field, otherwise the device is known as passive. The research has been carried out by taking three applications as examples, with respect to these examples, the authors have pointed out the possible threats. The main purpose of contactless tokens is to facilitate an active NFC device to retrieve the data stored in it. However, the Ticketing/Micro Payment application is used for transactions of any kind of information which generally includes more than one interface. Whereas, device sharing application of NFC is just used to establish the link between two communicating devices because due to the small bandwidth it cannot transfer images.

Eavesdropping is an issue of concern since the communication takes place by commuting through RF waves. In general, passive communicating devices are more secure than active passive devices. The exact proximity till which the attacker can eavesdrop cannot be determined since it depends on a number of factors, but it can be approximately concluded that in active mode it is possible till 10m and this is reduced by a large amount when passive mode is considered (about 1m).

Data corruption is a type of Denial of Service attack, where the attacker can easily manipulate the data so the receiver would not receive the correct information. This is often done by sending valid frequencies, so that the receiver is not able to understand the message the sender wants to transmit.

Data Modification the data revived by the receiver is valid but the data received is manipulated.

Data Insertion is the process of inserting messages between two communicating devices.

Man-in-the-Middle-Attack is impossible to be mounted in a real life situation. In this kind of attack, basically there exist two communicating parties, say Alice and Bob and a third unknown party say Eve establishes a link with Alice and a link with Bob. So when Alice tries to send any data to Bob, if Eve is close to Alice, it would receive the data and then generate a new RF field to send data to Bob. Since it is not possible for the 2 RF fields to be aligned properly together, the data received by Bob will be corrupted.

The possible solutions to the above mentioned problems can be:

Eavesdropping can be avoided by making a secure channel. The problem of data corruption can be solved by checking the RF field, while the data is being transferred. The problem of Data Modification can also be dealt best and most efficiently with a secure channel, whereas the problem of Data Insertion can also be tackled in the same way. To deal with Man-in-the-Middle attack we should try to use an active passive communication mode so that one of the trusted communicating devices can generate the RF field, which can be monitored by the active device to check for any disturbances or issues. To deal with any kind of attacks on the security, we could implement the concept of Secure Channel for NFC. A symmetric key is derived from the shared secret between two communicating devices. The shared secret can be established by any standard key arrangement protocol.

In the research carried out by Hussein Ahmad Al-Ofeishat and Mohammad A.A.AL Rababah they throw light on the concept of NFC, various modes of operations and on many real-time applications and how they are beneficial. The main advantage of NFC over other existing technologies of data communication is that there is no need to set up any kind of link between the communicating devices, the data can be transferred between two devices by simply bringing them in contact with each other. The only requirement is that the two communicating devices should have NFC. Based on the kind of usage we can categorise the applications into three main parts: Service initiated category where the information read by the NFC device from the tag is used for various other purposes, the next category is Peer-to-Peer category where between the two communicating devices a direct link is set up, the third and final category is the Payment and Ticketing where we can load virtual money in an electronic device like a cell phone. The conclusion drawn from this paper is that though the concept of NFC can make a huge impact on our lives, it is not fully developed to be used for business purposes and is still in the evolving phase. There are various security threats and it is very vulnerable to carry out secure transactions. The research work also suggests that we can implement various cryptography and encryption techniques in accordance with the type of environment to overcome the security issues.

In the work carried out by K.Preethi, Anjali Sinha and Nandini the main object was to put forward a comparison between all the existing techniques used for communication between two networking devices, it moreover illuminates the potential of NFC and how it could be used more in real-life scenarios. It brings up the possibility of how NFC can be used with other radio techniques or communicating techniques to be more efficient and secure. For example, we can consider the combination of NFC and Bluetooth, both being used together. Where NFC can be used to create the link and Bluetooth and be used for the transfer. So despite of the security threats and vulnerabilities of NFC, the research paper views NFC as a compliment to the existing technologies, which when paired with it can improve both the reliability and the speed. NFC has a very large scope as if implemented properly even a non-technical person can use it easily.

In the research done by Vibhor Sharma, PreetiGusain and Prashant Kumar the main objective highlighted here is the comparison of NFC with Bluetooth and the possible security threats that can be faced in NFC. NFC proves to be more beneficial than Bluetooth if the devices are in close proximity and it moreover allows the communication of data in both the directions rather than unidirectional flow of data as in case of Bluetooth. In addition to this the data transfer of Bluetooth is slower than NFC. One major drawback of NFC over Bluetooth usage is that large amount of data cannot be transmitted here. Kenya is adopting the technology rapidly and it has huge scope in the future because it makes the transactions easier for the user in addition to the less amount of time taken. The major step to be taken in order to create vast use of NFC is to create a secure platform so that the data transferred is valid and genuine.

The research written by Andres Diaz Lantada, Carlos Gonzalez Bris, Pilar Lafont Morgado and Jesus Sanz Maudes a new system has been proposed which gives us an application of NFC in medicine. According to the new idea, we can monitor various bruxism events and it also helps in the diagnosis. To carry out this application, a magnetic field with low frequency is generated by the reader and since the biological tissues cannot absorb low

frequency magnetic field, there is an advantage over Bluetooth based systems. The basic concept behind this idea is that a low frequency magnetic field is generated by the analogue front end due to which some value of voltage is induced in an LC circuit. The voltage used is always rectified and the rest of the system is provided power by this. There are two different subsystems present in the splint which is made by the integration of Passive sensor. The first subsystem can also be called as a power subsystem which has the following components: a low dropout regulator which can be used to provide us with a constant DC voltage, a Schottky diode rectifier and a LC circuit. The value of the resonance is kept approximately 125Khz. The force-sensitive oscillator constitutes the second subsystems which have some passive components and a low power relaxation oscillator and a transducer which is made out of two layers of substrate. On each of these layer first there is a coating of any conductive material like silver which is then followed by a layer of "pressure-sensitive sink". It is always kept in mind that the transducer should be positioned on the splint so that the oscillation frequency can be calculated. When we use this device, the estimated amount of power consumed is around 250microWatts. The application can further be expanded to treat the damages before there is a condition of irreversible damage.

In the research carried out by Nurbek Saparkhojayev, Abyek Nurtayev and Gulnaz Baimenshina points out about the role of NFC in Independent and complete ACMS (Access Control and Management Systems) and to maintain student attendance and location in the institute. Many modules together form a system these modules are: server application, NFC reader, Controller and Smartphone application. There are two main parts in the system mentioned above which are registration phase and door lock/unlock phase. Now, in these two phases mentioned earlier there are two different data exchange to be carried out. This data exchange is divided into two sub phases. The first sub phase is initiated by the server. The second sub phase is initiated by the controller where it waits till the device is in the lost proximity. The main advantage of this is that whenever a smartphone is lost, there is no need to change the lock, the UID of the lost device can be simply deleted from the system. Therefore, it provides great ease and the end users consider is easy.

In the research carried out by Hongwei Du the main objective of the research paper was to explain the applications of NFC in m-commerce recently undertaken by various companies. In today's world people are dependent on technology, in particular m-commerce so Hongwei has tried to integrate m-commerce with NFC to make it easier for the end users. Google has also taken initiative to support and further explore this by the Google Wallet payments. Further, to facilitate easy transactions many credit card companies are also trying to work with mobile developers. To promote NFC Google has also made Goggle Wallet Payments downloadable in phones with NFC. Recently in 2012, PayPal has made possible to carry out transactions person to person. The major drawback here is that it is not compatible with iPhones. More applications include redemption of coupons; Goggle provides a platform to do this. With the advancement in various fields, it is also growing in the sector of social media and gaming. With more knowledge and development of NFC it has a huge future scope mainly it's advantages in healthcare and in developing "smart homes". It could help the visually impaired to find objects easily so that they can move around more easily. Deaths due because of wrong dosage of drugs could also be avoided through NFC if the doctors have a complete database of the drugs and its compositions then they could sync that with the patient database to avoid allergies or any kind of reaction with the drug. It has also been suggested that a kit could be developed for the post-surgical purposes which could manage and test the operated part for any kind of recurrence and thus avoiding any kinds of complications.

In a research carried out by Vedant Coskun, Busra Ozdenizci, Kerem Ok and Mehmet N Aydin provides an analysis between the different operating modes and draws a conclusion as to which one is the better among the others through a survey of 35 different applications. Out of which, 6 use Card Emulation mode, 29 use Reader/Writer mode and 2 use Peer to Peer mode whereas, two use both Card Emulation and Reader/Writer mode. In the case of Card Emulation mode, the data is present in the NFC devices, in case of Reader/Writer mode the data resides in the NFC tags and in case of Peer to Peer mode two communicating NFC devices are present. According to the analysis, the need to carry any kind of physical objects such as keys, credit cards is eliminated by Card Emulation method, whereas the Reader/Writer mode can be adaptive in different kinds of applications and is considered to be easiest to implement. On the other hand, the Peer to Peer mode allows the data to be transmitted easily between two connected devices.

In the research work carried out by Adam Mrarcus, Guido Davidzon, Denise Law, Namrata Verma, Rich Fletcher, Aamir Khan and Luis Sarmenta give a new idea on how medical facilities can be provided through NFC in a low resource environment. The lost cost of mobile phones makes it affordable for a lot of people. The main objective is to implement an idea which can be used mostly in the developing countries. The example used here is of Karachi healthcare system where they use this idea to detect pneumonia in children. This method has major drawbacks such as it is not reliable in terms of patient identification and in detecting the illness. This has been implemented by creating a phone with a patient presence alert system based on the concept of NFC and the enrolled patients will have an NFC card which would be scanned by the physician. The doctor would be then prompted to carry out the pneumonia diagnosis, if this comes out to be positive then the details of the patient would be sent out for further investigation and treatment by the specialised mobile team. There this concept is implemented using mobile phones because it presents an added advantage of the facility of Bluetooth. The interface has been made

user friendly that in case of lost or broken tags the physician can manually enter the patient's ID. The limitations of this application is that there is no backup in case when there is some problem in the cell phone further the patients should be reminded again and again that they do not exchange the tags because then their course of treatment will go wrong.

The following is a survey conducted on the near field communication by Anusha Rahul, UnniKrishnan, Gokul Krishnan and Sethuraman Rao. According to the survey conducted by them the NFC is one of the most recent and effective technology in wireless communication. Two devices can communicate through NFC by as simple way as pointing towards each other or touching each other. Though it has many advantages it also has many disadvantages like the short range it has to achieve or acquaint itself with. The communication is brought about in the NFC enabled devices only and within a theoretical range of 20cm only. But the technology does not require any net usage unlike other devices of communication. NFC though provides an innovative way for communication within two smart phones or any other device for that matter. This paper states that the NFC has the potential to provide an alternative and actually replace plastic cards used for the purpose of ticketing and banking with the smart phone advanced technology based on entirely on NFC. Now the technical facts say that NFC operates at around 13.56Mbps and 424kbps data transfer rate. The main advantage that NFC provides over Bluetooth communication is the power consumption and ability to communicate without pairing. But then again the highest data transfer rate is way less than that in Bluetooth communication (424kbps in comparison to 2.1Mbps).

Here is another paper describing the NFC in detail proposed by Vedat Coskun, Busra Ozdenizci and Kerem Ok titled 'A Survey on Near Field Communication (NFC) Technology. They state in the paper that NFC is a short ranged wireless technology that is going to be useful in the coming days and has an added advantage over other communication mediums. They have taken into account the business economics, ecosystem and tragic issues along with security issues into consideration in the following paper. Mobile phones have been already provided with numerous methods for communication like sms, mms, gsm communication etc. NFC thus provides a better and new concept of communication. This basically uses the touch paradigm. How exactly does user use this type of technology? The answer is simple-user interacts with a smart object first which mainly would be a NFC tag or NFC enabled device using his own NFC enabled mobile. The NFC enabled mobile then uses this information to search on the world wide web for instance and thus processes this information to generate more advanced and in depth information. RFID (Radio Frequency Identification) technology is the most important and basic part of NFC technology in mobile reading ability. Three different distinct types of NFC modes are defined and the communication protocols vary in each particular mode.

S. Kavaya, K. Pavithra, SujithaRajaram, M. Vahini, N. Harini proposed a vulnerability analysis for the NFC in this research paper along with security system for the NFC. They propose to use an encryption system for the NFC enabled applications using a combo of AES cryptography algorithm diffie-Hellman Key negotiation scheme. This paper points out to us that NFC involves inductive coupling technique where loosely coupled inductive circuits share their power within each other over a distance of few centimetres. At the initial stage the NFC protocol couldn't provide any reliable security. This research paper will enable us to make NFC more secure. The basic idea is to use cryptographic methods. But as mentioned these methods fail. Thus the new AES the successor of DES is used in the security purpose. The AES uses permutations and combinations which briefly involves a sequence of substitution and permutation steps to create an encrypted block. The other part then involves using the Diffie-Hellman algorithm. The algorithm involves selecting a prime number 'q' and a primitive element 'pe' by both the sender as well as the receiver. Sender then chooses the secret 's' and calculates $(pe^s) \bmod q$. Receiver on the other hand chooses secret 't' and calculates $(pe^t) \bmod q$. Both these calculated values are then exchanged with each other and the key is thereby computed.

There is a paper proposed by Gauthier Van Damme and Karel Wouters which records the practical experiences with the NFC security on the mobile phones. The possibilities of NFC applications on today's technology are illustrated in the paper. We know that the security protocols are PKI-based and as a result actual slowdowns are not only caused by the extensive use of cryptography but also by the design decisions that the mobile phone manufacturer takes. As mentioned earlier the NFC has three modes of communication. The NFC though can communicate in either an active way or a passive way. These are included in the standards of NFC. The three modes are- 1) Card Emulation Mode 2) Reader/Writer Mode 3) Peer to Peer Mode. The security issues are also discussed in detail in this paper. Eavesdropping, Data Modification and Man in the middle are the three types of security issues that the NFC will face. The practical experiences do not obey the theoretical conjectures. The heavy cryptography being used along with the relative immaturity in the availability of NFC phones increases the ideal transaction time in a NFC based online transaction.

Garima Jain and SanjeetDahiya have prepared a thesis explaining the advantages, limits and the scope of NFC technology. They have stated that NFC can be the next generation RFID as the basic working principle of the NFC technology is completely based on the RFID but considering the application perspective it can be correlated to Bluetooth as it regulates communication between two active devices. One of the advantages of NFC is that it provides bi-directional communication for exchanging data which means both the devices can simultaneously send and receive information. NFC is assumed to consume less power in comparison to other wireless

communication methods. NFC does not need any connection to be set up to get it working so it becomes easier to use it in crowded areas. NFC components can be integrated on one chip device. Along with the various advantages NFC also has certain limits and challenges. Lack of information is one such limit. Security in NFC can be an issue as radio waves are being used for transfer of data. Some useful applications of the NFC include Contactless Payment, Keeping Records, Transit and ticketing, Automated Check-in System, Advertising etc.

This is a research paper submitted by Ben Dodson, Hristo Bojinov and Monica S. Lam stating the touch and run technology using the NFC. They state that NFC allows for contextual application innovation (CAI) which results in execution of code on our smart phones as a result of our environment. The paper then presents a number of applications using CAI and addresses the associated security and usability concerns. Availability of NFC on the smart phones can be an exciting feature for various designers as it programmatically generates new information. Various applications on phone have been devised using the NFC technology. A transaction attachment is a class of useful applications that can be classified as attachments. The applications can be classified into three further categories depending on CAI used- attachments to transactions, virtual token for replacing the real-life world token and junctions for connecting peer-to-peer applications on mobiles. Security threats in the NFC technology are known to us quite well by now. The phone nowadays holds increasing amounts of private important data. Loss and protection of device thus becomes a prime concern. Thus NFC shows us that the applications can be run as side-effect of some other arbitrary transaction. One phone thus can provide context to another to create and thus successfully create a junction between the devices.

Lawrence Muriira and Nimrod Kibua put forward an idea which they claim to be the Kenya's future mobile money service using the NFC technology. They claim that the devices running on the mobile platform can be converted into mobile payment systems. Different modes of payment solutions are being used all over the world. The main objective was to study the feasibility of the common and primary modes of mobile networks which include SMS based transactional payments, mobile billing, mobile online payments and most promising is the future further opportunities of NFC. The mobile companies have started to build their own mobile phones which are equipped with NFC. The NFC technology has come into notice with big ICT and telecom industry players. The technology can actually build a mobile wallet cash. This will definitely help the users of Kenya to carry out certain transactions easily without any harm. Also survey also tells that more than half population of Kenya uses smart phones. They explain the scope of the NFC by using within the transport sector due to its high number population.

Vibhor Sharma, Preeti Gusain and Prashant Kumar have proposed a paper in the topic of near field communication in which they have discussed the fundamentals of the NFC technology. A brief analysis between NFC and Bluetooth is done. NFC can work in active as well as passive mode. The functionalities though are different. The data transfer rate is higher

In NFC as compared to any other Bluetooth device. In Bluetooth a manual connection needs to be established within two devices each having Bluetooth facility whereas in NFC we do not need to manually establish connections. The connections are automatically joined. But again the NFC technology fails in the security issues. If the NFC enabled device happen to be stolen then the thief can swipe in front of the card reader and make transactions however strong the encryption might be. Various protection measures are being invented or designed in order to avoid this security failure. Kenya has completely adopted the NFC technology. Thus, NFC will enable users to carry out transactions on mobile phones simply by tapping the screen or mobile or device for that matter with the card you wish to use.

Ernst Haselsteiner and Klemens Breiffuss have proposed a paper underlying the strengths and weaknesses of the NFC technology. It mainly focusses on security in the NFC. When the NFC device is in active mode it sends data using the amplitude shift keying. In passive mode the data will be generally transferred using a weak load modulation. The data is then thus always encoded using the manchester coding. The major threats faced include Eavesdropping, Data modification and data corruption. NFC key-agreement mechanism was introduced in this paper in order to provide cheap and fast secure key agreement. The typical use cases of the NFC interfaces were also introduced in this paper. Some of the applications of the secured NFC include contactless token, ticketing/micro payment, device pairing etc. This paper also contains a brief explanation of the man-in-middle attack. It is nothing but when two people having a conversation and a third person comes in between the two disrupting their conversation and having his own conversation with each of them. This sort of attack is called the man-in-middle attack.

In the following paper, Adithi Kiran Bandarkavte, Jagadeesh Sai. D have proposed a new methodology for secure healthcare monitoring system using NFC technology. Mobile nowadays has become handier and is available to almost every common man. This important fact can be used to our benefit by making use of it in the medical sector. A simple tap is all what will be needed to say check your records or your whole previous medical history and what not. They have proposed the same extension of this idea in this research paper. The advantages of this technology will be that it will enable proper and accurate time to time diagnosis of the patients with minimal effort. Like for example in an emergency test the doctor has to start all the tests from the scratch and carryout his analysis and accordingly prescribe the medication. But by using this technology we can ensure that the records

are stores in a proper database and easily accessible as NFC involves just a tap. Thus this paper suggests a new innovative way in medical field for better performance and accuracy.

In the research performed by Diego, the main emphasis is on the NFC and CAP compatibility. Major components used in this mechanism are NFC and CAP (Chip Authentication Program).

The document by Diego will focus in the security aspects of the MFC-CAP solution. Section 2 has explained the entire working of NFC-CAP, Section 3 enumerates the threats, Section 4 highlights the drawbacks particularly the attacks and Section 5 countermeasures taken to abolish these attacks.

Drawback of Diego's results conclude that passive attacks occur when the attacker can only listen to the information and active attacks may occur when the attacker has the access to edit, modify and remove the data. Some expected threats:-

PIN REVEALATION

The PIN is handled by 4 Principals-User keeps secrecy of the PIN, Card protects the PIN and to no leak it. Attacker replaces the genuine card with a malicious card and keeps the PIN for later retrieval.

USER IMPERSONATION

Attacker impersonates the user to the bank and fools the bank to think that he is an authenticated user while actually he is not. An active attack targets the PC or Channel B is common to PCR based and phone based CAP. Busra's research emphasizes on Indoor Navigation Systems which is the emerging topic today since GPS signals lack indoor. NFC internal enables a user to navigate through some arena by enabling a 'location-update', by simple tapping the NFC tags which diverge out and orient the user to his aiming position.

Busra has skilfully presented all his ideas into this journal and has partitioned it aptly based on the structure, requirements, drawbacks and advantages.

The concepts majorly used will be summed up as:

- 1) Technologies regarding positioning and enabling indoor as well as outdoor navigation.
- 2) NFC technology, its modes of operations and issues combined.

In the work performed by Michael Roland, his purpose is to emphasize the use of Software card emulation. The technology is latest in the field of NFC enable mobile phones and aims at operating and simplifying the complex card emulation functionality. First introduced in Research in motion(RIM) by Blackberry phones. This particular form of card emulation removes the secure element of the phones thus making the card emulation hampers with the security issues and makes a way in for the attackers around.

Michael's work depicts the pros and cons of software card emulation (SCE) that is based on the existing scenarios. The secure element is a microchip embedded into the NFC device. Or maybe it is integrated with other smart cards that are used into the NFC device. Secure elements can be used through a contact or a contactless medium. The major difference being the interface they provide. Secure elements provide secure storage, friendly execution platform, hardware based support for cryptographic assignments. They have a firewall to protect them against attackers. Embedding severe elements usually keeps it under control of the manufacturer or the manager of services. Software card emulation (SCE) mode is used to communicate NFC enabled devices that do not have proper peer to peer mode. Reader/writer support for contactless smartcards is well maintained with the PC and integrated into almost all of the Operating system environments.

The research by Nikolas Alexio show that NFC enabled devices thus can communicate through a wireless environment just through a tap contact. Since the attacks are capable to bypass the NFC requirement for less distanced communications easily hence it becomes vital to analyse the security measures of NFC links. The research here shows a general perspective and a formal analysis of verifying the NFC protocol against relay attacks. Towards the end, the researcher has built a time marcov chain model using a PRISM model checker. Initially NFC protocol parameters are taken into consideration and then the model is enhanced with networking parameters that includes both the mobile environment and security checked characteristics. Relay attacks are kind of man-in-the-middle attacks. A malicious player with no knowledge of protocols could hack through the communication between the 2 parties by challenging them through a virtual platform. The attacker is capable of hijacking the authentication protocol by putting a legit challenge, which will inform him with all the appropriate information and rules that can further be given back to the verifier. The research has given an approach that will examine the security of NFC and that can be used to aid the conflicting NFC applications. The journal's results show that a thin time out timer while the data exchange process happens, volume of the data and size of packets between the 2 parties and a high error rate on the communication channel which can majorly reduce the estimated probability of a relay attack.

Dino Zupanovi's research has proposed ferry ticketing system based on NFC. The Four major topics are broadlyelaborated in this journal stating facts and specifications of ferry lines and benefits of implementations of such solutions being NFC specifications, NFC ferry ticketing logic, NFC security issues and discussions about pros and cons that are possible in this field. The utmost objective of the journal is to present possibilities of using NFC technology to practise in ferry ticketing system module circumfering Croatian ferry lines specifications.

Concerns expressed by the researcher in the ferry ticketing field-To ensure your NFC communication is completely protected, it is checked that once the destination reaces the favoured ferry port and begins the DFT

authentication NFC port and FPOS port, certain security measures should be fed in the communication logic between the destined user and FPOS NFC port. This particular step is essential as it assures an extra security layer for NFC about it being a wireless technology that might not be able to sustain wireless attacks.

Out of the numerous schemes that focus majorly on transaction security and not user's security, work of Jia Ling proposes and Unlikeable Anonymous payment scheme so as to circulate a secure as well as an anonymous mobile commerce platform. According to his proposal, the user applies a virtual based credit card from a trusted service manager. All the delicate credentials of the particular credit card are kept in the secure element of user's device. The proposed journal has numerous advantages some being anonymity and non-repudiation etc.

The research is broadly classified into 4 major parts and elaborated below:

1. Registration phase: here, the system generates parameters that will be needed during the payment procedure
2. Anonymous virtual bank account generation phase: the user keeps a proposal for a bank account for payment.
3. Anonymous transaction account generation phase: the user takes the identifier from his virtual bank account in order to create a transaction account.
4. Virtual credit card generation phase: A user pleases for a temporary virtual based credit card and stores it for later use.

In the research done by Soon-Nyeon Cheong, his major focus lies with the revolutionary and the deadly usage of smartphones in today's era life has become much easier. Be it the storage capabilities, fast computing, portability talents. Usage of NFC into the smart phones has opened even more opportunities for new models. NFC and graphical password methods which are the 2 outstanding and independent technologies that are used to achieve secure and easy access to control systems. A very secure NFC ESGP device access control system for unlocking a particular door is also demonstrated. This system allows its users to access the digital key that is saved in their NFC enabled device to use it easily throughout the ESGP scheme.

Two major processes involved are – The registration Process and The encoding process.

The user's image in any form is captured during the registration process and this is chosen to be the host photo for the generation of stegno-photo in the later stage. A graphic key is chosen further which is an asymmetric cryptographic algorithm. The stegno-photo is obtained by embedding the host photo with the encrypted passcode using 'steganography'.

This journal work uplifts the expectations of technological capabilities by making a new better and a secure NFC ESGP access control platforms, letting users to easily and safely use their NFC device as a key to access the control system.

IV. CONCLUSION

In the research carried out we have tried to analyse NFC technology, its working and its advantages and disadvantages from the various research papers published related to the above topic which is Near Field Communication (NFC). NFC has a lot many scopes in future because it makes it easier for the end users to use the technology efficiently and accurately. Though there are some security issues in the implementation to get valid data, there is research going on in various areas as how it can be implemented in fields of Health Care, Housing, making payments, institutional and educational purposes. The corporate industries like the credit card companies are trying to merge with mobile development companies to implement the concept of NFC, so that payment can be made without having the need to carry wallets. There is a high scope in this area of technology that can bring a huge change in our day to day lives. Companies like Google and PayPal have started using this technology.

V. REFERENCES

- [1]. Haselsteiner, E., & Breituß, K. (2006, July). Security in near field communication (NFC). In *Workshop on RFID security* (pp. 12-14).
- [2]. Al-Ofeishat, H. A., & Al Rababah, M. A. (2012). Near field communication (NFC). *International Journal of Computer Science and Network Security (IJCSNS)*, 12(2), 93.
- [3]. Preethi, K., & Sinha, A. (2012). Nandini," Contactless Communication through Near Field Communication. *International Journal of Advanced Research in Computer Science and Software Engineering*, 2(4).
- [4]. Kostakos, V., & O'Neill, E. (2007, March). NFC on Mobile Phones: Issues, Lessons and Future Research. In *PerCom Workshops* (Vol. 8).
- [5]. Du, H. (2013). NFC technology: Today and tomorrow. *International Journal of Future Computer and Communication*, 2(4), 351.
- [6]. Saparkhojayev, N., Nurtayev, A., & Baimenshina, G. (2014). Access Control and Management System Based on NFC-Technology by the Use of Smart Phones as Keys. *Middle-East Journal of Scientific Research*, 21(7), 1130-1135.
- [7]. Coskun, V., Ozdenizci, B., & Ok, K. (2013). A survey on near field communication (NFC) technology. *Wireless personal communications*, 71(3), 2259-2294.
- [8]. Ok, K., Aydin, M. N., Coskun, V., & Ozdenizci, B. (2011). Exploring underlying values of NFC applications. In *3rd International Conference on Information and Financial Engineering IPEDR* (Vol. 12).
- [9]. Riyazuddin, M. (2013). NFC: A review of the technology, applications and security. *ABI research*.
- [10]. Sharma, V., Gusain, P., & Kumar, P. (2013). Near field communication. *Department of Computer Science & Engineering Tula's Institute, The Engineering and Management College, Dehradun, Uttarakhand*, 248001.
- [11]. Ortiz-Yepes, D. A. (2009). NFC-cap security assessment. *IBM Research GmbH, Zurich, Security Assessment RZ*, 3736.
- [12]. Ozdenizci, B., Coskun, V., & Ok, K. (2015). NFC internal: An indoor navigation system. *Sensors*, 15(4), 7571-7595.
- [13]. Roland, M. (2012, June). Software card emulation in NFC-enabled mobile phones: great advantage or security nightmare. In *Fourth International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use* (pp. 1-6).

- [14]. Alexiou, N., Basagiannis, S., & Petridou, S. (2016). Formal security analysis of near field communication using model checking. *Computers & Security*, 60, 1-14.
- [15]. Zupanovic, D. (2015). Implementation model for near field communication in croatian ferry ticketing system. *Procedia Engineering*, 100, 1396-1404.
- [16]. Luo, J. N., Yang, M. H., & Huang, S. Y. (2016). An Unlinkable Anonymous Payment Scheme based on near field communication. *Computers & Electrical Engineering*, 49, 198-206.
- [17]. Cheong, S. N., Ling, H. C., & Teh, P. L. (2014). Secure encrypted steganography graphical password scheme for near field communication smartphone access control system. *Expert Systems with Applications*, 41(7), 3561-3568.
- [18]. Burkard, S. (2012). Near field communication in smartphones. *Master Student, Computer Engineering Dep. of Telecommunication Systems, Service-centric Networking, Berlin Institute of Technology, Germany*.
- [19]. AlZuhair, M. S., Najjar, A. B., & Kanjo, E. (2014, July). NFC based applications for visually impaired people-A review. In *Multimedia and Expo Workshops (ICMEW), 2014 IEEE International Conference on* (pp. 1-6). IEEE.
- [20]. Want, R. (2011). Near field communication. *IEEE Pervasive Computing*, 3(10), 4-7.
- [21]. Pavlopoulos, S., Kyriacou, E., Berler, A., Dembeyiotis, S., & Koutsouris, D. (1998). A novel emergency telemedicine system based on wireless communication technology-AMBULANCE. *IEEE Transactions on Information Technology in Biomedicine*, 2(4), 261-267.
- [22]. Coskun, V., Ozdenizci, B., & Ok, K. (2015). The Survey on Near Field Communication. *Sensors*, 15(6), 13348-13405.
- [23]. Kavya, S., Pavithra, K., Rajaram, S., Vahini, M., & Harini, N. (2014). Vulnerability Analysis And Security System For NFC-Enabled Mobile Phones. *International Journal of Technology Enhancements and Emerging Engineering Research*, 3(6), 207-210.
- [24]. Francis, L., Hancke, G., Mayes, K., & Markantonakis, K. (2010). On the security issues of NFC enabled mobile phones. *International Journal of Internet Technology and Secured Transactions*, 2(3-4), 336-356.
- [25]. Van Damme, G., Wouters, K., & Preneel, B. (2009). Practical experiences with NFC security on mobile phones. *Proceedings of the RFIDSec*, 9, 27.
- [26]. Dodson, B., Bojinov, H., & Lam, M. S. (2010). Touch and Run with Near Field Communication (NFC).
- [27]. Ozdenizci, B., Alsadi, M., Ok, K., & Coskun, V. (2013). Classification of NFC Applications in Diverse Service Domains. *International Journal of Computer and Communication Engineering*, 2(5), 614.
- [28]. Muriira, L. M., & Kibua, N. (2012). Near Field Communication (NFC) Technology: The Future Mobile Money Service for Kenya. *International Journal Of Computing & ICT Research*, 6, 1, 73-83.
- [29]. Ozdenizci, B., Aydin, M. N., Coskun, V., & Ok, K. (2010, June). NFC research framework: a literature review and future research directions. In *The 14th International Business Information Management Association (IBIMA) Conference. Istanbul, Turkey*.
- [30]. Jain, G., & Dahiya, S. NFC: ADVANTAGES, LIMITS AND FUTURE SCOPE.