Internet of Things: Machine to Machine communication with emphasis on role of RFID and NFC

Jinisha Bhanushali, Piyush Dinde, Shreya Chakraborty

Abstract—Internet of Things (IoT) is a concept which, for quite a while now, has been identified as the future of internet. It has opened up new possibilities for the implementation of smart environments. Machine-to-machine communication technologies like WiFi, Bluetooth, Radio Frequency Identification (RFID), Near Field Communication (NFC), etc. play a pivotal role in Internet of Things. This paper highlights the function of device communication in terms of IoT and compares the technologies based on different parameters. Our main purpose is to focus on the usability of RFID and NFC technology for machine communication. Through this paper, we aim to point out the features and future scope of both RFID and NFC which make them perfectly suitable to serve the purpose of device communication in the large scale implementation of Internet of Things in near future.

Index Terms—Internet of Things, Machine to Machine, NFC, RFID.

1 Introduction

The Internet of Things (IoT) is a recent communication paradigm that envisions a near future, in which the objects of everyday life will be equipped with microcontrollers, transceivers for digital communication, and suitable protocol stacks that will make them able to communicate with one another and with the users, becoming an integral part of the Internet [1]. It is a multidisciplinary topic that includes a range of subjects ranging from technical issues (routing, queries) to a combination of technical and societal issues like security, privacy and business ethics. The efforts of the early researchers to create a common interface between technology and everyday life resulted in the creation of Internet of Things. As Mark Weiser states "the physical world is richly and invisibly interwoven with sensors, actuators, displays, and computational elements, embedded seamlessly in the everyday objects of our lives, and connected through a continuous network". IoT pointed out the use of RFID, sensors, new nanometer materials, embedded systems and other technologies, all the things in the world can exchange information through interconnection networks [2].

In order to make the scheme of IoT work, a very important prerequisite is to master the device communication (Machine-to-machine communication) technologies. Currently, many such communication technologies like WiFi, Zigbee, Bluetooth, Near Field Communication (NFC), Radio-Frequency Identification (RFID), etc. are being used at preliminary levels in many small scale applications. To imagine a huge network of things, it is essential to recognize the potential scopes of all these technologies and identify the ones that are worth investing our resources. With its major focus on RFID and NFC technologies, our paper takes into consideration the basic characteristics these technologies possess and the ones they need to fulfil to find a noteworthy place in the future implementation of Internet of Things.

RFID technology has been around for a long time now- be it for the access control to enter the office, library ,in retail stores, in consumer electronics like smart phone ,in security systems and many more. Comparatively, NFC is a newer concept which is a mere subset of RFID. Both these technologies use the RF field for communication, identification, access control, etc. It might look like NFC would soon substitute RFID in many applications. However, it is important to note that NFC works on short range communication and RFID has a much larger range. Therefore, both can be thought of as complementary technologies where one works on the weaknesses of the other. This paper merely intends to speculate the capabilities of these technologies for making the dream of Internet of Things come true.

- *Jinisha Bhanushali is currently pursuing bachelor degree program in electronics engineering in Mumbai University, India, PH-+917715909022. E-mail: jinishabhanushali29@gmail.com*
- *Piyush Dinde is currently pursuing bachelor degree program in electronics engineering in Mumbai University, India, PH-+919619935657. E-mail: piyushdinde@gmail.com*
- *Shreya Chakraborty is currently pursuing bachelor degree program in electronics engineering in Mumbai University, India, PH-+918108535900. E-mail: shreyasriparna1809@gmail.com*

2 Requirement Of IoT Environment

The most basic and necessary feature of IoT is the use of smart objects. For the realization of this concept, it is required that the objects are able to perform basic functions of sensing and processing various physical or ambient phenomena and generate varying automated responses according to the inputs. This can be done by making use of embedded processing

techniques with the help of micro-controlled units embedded in all the objects around us. Machine-to-machine communication is the concept designed to provide this very purpose of sensing, processing, programmability and deterministic command and control functionality by enabling communication between the sensing nodes and processing nodes at different destinations within the system. In addition, to be able to handle the sheer number of things and objects that will be connected in the IoT, cognitive technologies and contextual intelligence are crucial [3]. Also, cloud computing has been identified as another vital feature for the future Internet of Things. The fusion of cloud computing and Internet of things will open up several opportunities in the IoT services field. Further, with increased number of devices connected through the internet, the need of increasing the address space will arise. Therefore, with a transition towards IPv6, there will be virtually unlimited number of public IP addresses which will have the provision to connect billions of devices within several layers of interconnected networks.

3 Machine-To-Machine Communication

Machine-to-machine (M2M) communication forms the basic framework for an IoT system. It takes its roots from the concept of telemetry which has been conventionally used for remote sensing and real time data acquisition in science and technology applications. However, through the deployment of M2M in IoT, it forms an extension into a more generalized application pool including traffic control, warehouse management, automatic systems, etc.

Machine-to-machine communication is the essential principle behind the communication between the devices connected within an IoT network. It provides sensing, identification, interaction and cooperation between objects or devices. Basically, it is this concept that makes IoT workable. The inputs to such a system are real time coefficients collected from the physical world which can be interpreted electronically by the devices themselves to provide corresponding responses, thereby granting efficiency and optimization of processes. This requires conversion of all the devices from independent non-connected devices to smart devices. After a device becomes smart through the integration of embedded processing, the next logical step is remote communication with the smart device to help make life easier [4]. This is done by incorporating them into a vast network of things using embedded technology in which they can communicate within themselves and allow automation without human intervention. Current M2M manufacturers have been integrating Internet-connected systems into high-value asset tracking, alarm systems, fleet management and the like for more than 15 years. [5] As IoT makes its way into the cursory applications for personal as well as general use, it will require a common basic M2M communication platform for efficient device communication.

To understand the role that M2M plays, it is germane to specify the technologies which would be required to complement an M2M communication to allow flexibility and efficiency of the IoT networks. In general it can be described as a system made up of sensors networks, internet connectivity and communication strategies like RFID, Bluetooth, NFC, etc. The interdependence of these essential blocks enables simple passive objects to become "smart" devices, making automation of tasks possible. The ability to react to events in the physical world in an automatic, rapid and informed manner not only opens up new opportunities for dealing with complex or critical situations, but also enables a wide variety of business processes to be optimized. [6]

4 M2M Communication Technology

Efficient device identification and communication provide a base for implementing an M2M framework. The emergence of many potential communication technologies has proved to be a major advantage in designing such systems. Some of the technologies which might be useful for this purpose are Radio frequency identification (RFID), Near-field communication (NFC), WiFi, Zigbee, GPS, Bluetooth, Information and Discovery Service (IDS), Barcodes, Supervisory Control and Data Acquisition (SCADA), etc. Table below shows the features of some communication technologies which make them potential strategies for implementation of machine communication. The feasibility of each of these technologies in the future will decide their usability for deployment of widespread M2M communication networks in the ubiquitous IoT.

TABLE 1
MODES of M2M COMMUNICATION

Technology	Power Usage	Range	Latency	Cost
Zigbee	Moderate	30-100m	20msec	Moderate
Bluetooth	Moderate	10m	6sec	Moderate
RFID	Low	3m	<1sec	Low
NFC	Low	<0.1m (usually 10cm)	<0.1sec	Low

4.1 RFID

Radio Frequency Identification (RFID) is a way to identify objects and transfer data by using radio frequency tracking tags or frequency electromagnetic fields. The concept of RFID is relatively old but recent advancements in chip manufacturing have made it possible to use it for practical applications in consumer level tagging revolutionizing the supply chain management. One of the earliest applications of RFID was in 'Identify Friend or Foe' (IFF) system deployed by the British Air

Force during the Second World War. The IFF allowed the pilots to differentiate between friendly aircrafts and hostile aircrafts by the use of RF signals.

The main components of RFID system include tags, readers, antenna and host computer with corresponding appropriate software application. RFID tags are basically integrated circuits of extremely thin (as thin as 0.3mm) and tiny microchip of capacity 64 bits with a coupling element which is in most cases an antenna coil. The data is stored within a tag's microchip. RFID tags contain at least two parts: an integrated circuit for storing and processing information, modulating and demodulating a radio-frequency (RF) signal, collecting DC power from the incident reader signal, and other specialized functions; and an antenna for receiving and transmitting the signal. The tag information is stored in a non-volatile memory. The RFID tag deploys either programmable or fixed logic for processing of the sensor data and transmission. A tag acts like a transponder and is programmed with all the information about the substrate on which it is mounted. RFID tags recognize a radio signal by the RFID reader i.e. it receives a query, and immediately responds by sending its data to the reader. There are 3 types of tags based on power source; active, passive and semi passive. The active tags have their own source of power and are capable of initiating communication to the reader or other tags. The passive does not have its own power source whereas a semi passive tag may possess an internal battery but is incapable of initiating communication.

TABLE 2
COMPARISION OF PASSIVE, ACTIVE and SEMI PASSIVE TAGS [7]

Passive	**Semi Passive**	**Active**
Uses RF waves as power source	Battery	Battery
Not expensive	Moderately expensive	Very expensive
Range of distance in tens of meters	Range of distance around 100 meters	Range of distance above 100 meters
Capable of only response	Capable of only response	Capable of response and communication
Used in Electronic Product Code cards	Electronic tolls	Asset tracking

RFID systems can be classified based on the type of reader and tag. A Passive Reader Active Tag (PRAT) system consists of a passive reader capable of receiving radio signals from an active tag only. The range of this system is flexible and can be as high as 2000 feet. An Active Reader Passive Tag (ARPT) has an active tag that receives and transmits signals from a passive tag only. Active Reader Active tag (ARAT) system uses active tags which can only be awoken with an interrogator signal from the active reader. RFID readers communicate with the RFID tags via RF channel to obtain identifying information. For simultaneous multi tag reading the reader may have to employ an anti-collision protocol to avoid data over riding and conflicts. Readers are also used to power up passive data tags which have no power source and depend on the reader to decode. Readers may be of many types operating on many frequencies with a wide range of functionalities possessing their own power and internal storage and offer network connectivity.

RFID systems operate at various frequencies depending on their application. The operation frequency determines the physical materials that will propagate the RF signals. Tags operating at ultra high frequency (UHF) are not suitable for proper working in close proximity to liquids and metals. Different sizes and shapes of RFID antenna operate at different frequencies. The frequency ranges for RFID tags and their read distances have been listed in the table below [7]:

TABLE 3
FREQUENCY RANGE of RFID TAGS

Frequency Range	**Frequencies**	**Passive Read Distance**
Low Frequency (LF)	120-140 KHz	10-20 cm
High Frequency (HF)	13.56 MHz	10-20 cm
Ultra-High Frequency (UHF)	868-928 MHz	3 meters
Microwave	2.45 & 5.8 GHz	3 meters
Ultra-Wide Band (UWB)	3.1-10.6 GHz	10 meters

(from RFID (Radio Frequency Identification): Principles and Applications ,Stephen A. Weis,MIT CSAIL)

Electronic Article Surveillance (EAS) tags are the most basic passive tags that just ascertain the presence of the product to the reader. EPC tags can be passive, semi passive or active having real information regarding the product like a unique code and can be used for tracking application. Sensor tags may have an onboard sensor that senses the surrounding parameters and automatically logs in and stores the data. Smart dust Motes are capable of initiating their own communication with other devices forming ad hoc networks and are most necessarily active tags.

They are much more complex than simple EPC-style RFID. Research on smart dust is being conducted in University of Berkeley and Intel.

RFID style tags have been divided into 5 classes from class 0 to class 4 by EPC global [8]. These tag functionality classes are summarized as below:

TABLE 4
TAG FUCTIONALITY CLASSES

Class	Name	Memory	Power Source	Feature
0	EAS	None	Passive	Article Surveillance
1	Read only EPC	Read only	Passive	Identification Only
2	EPC	Read /Write	Passive	Data Logging
3	Sensor Tags	Read /Write	Semi-Passive	Environmental Sensors
4	Motes	Read /Write	Active	Ad Hoc Networking

The main feature of RFID is the ability to read and write data without direct contact outside the line of sight like reading on conveyor belts, access control passes, ticketing and tracking and many more with the help of electric and electromagnetic wave transmission. It provides error free wireless data transmissions both battery free and maintenance free. The combination of product with its information has been phenomenal in the case of reliable system configuration and communication. RFID ensures the possibility of having unique identification lessening the chances of duplicacy and counterfeiting thereby guarantying security to sensitive data. In addition to the above high speed data capture of about 10 ms per tag in process control asset tracking application and simultaneous multi tag reading are also some of the features of RFID. High tech RFIDs may read about 10 to 50 tags per second. They have applications in supply chain management, library, apparel and fast inventory manufacturing units to keep count. Also, RFID tags are being widely used for tracking consumer products across the world. They are loaded with important information regarding the product for example, its warranty information, manufacturing details,cost and so on. RFID systems can work faultlessly even in extreme temperatures and harsh environments in presence of dust and dirt which makes them quite robust and perfect for applications in large scale implementation of IoT networks.

RFID miniaturization has made it easy to incorporate and conceal it in many day to day items. For instance the researchers in Bristol University in 2009 have successfully glued RFID micro- transponder to live ants in order to study their behaviour [9]. Currently Hitachi holds the record of the smallest RFID chip in the world of dimension 0.05mm x 0.05mm [10]. In 2014, the world RFID market is worth US$8.89 billion, up from US$7.77 billion in 2013 and US$6.96 billion in 2012. The market value is expected to rise to US$27.31 billion by 2024 [11]. This includes tags, readers, and software/services for RFID cards, labels, fobs, and all other form factors.

With major advancements on its way, RFID is all set to boost the growth of machine to machine communication (M2M) and machine to object communication (M2O) with the help of high tech RFID enabled sensors and RFID transponders. Passive RFID tags which do not require power source, operate on the energy given out by the reader's antenna's Radio frequency (RF) field and don't require batteries or maintenance. However RFID is not without its own share of demerits. RFID Tags and Readers may not work properly due to the problem of interference with other wireless devices. It also lacks in proper security of personal or sensitive data. Overcoming these problems is a difficult task. A lot of work will be needed to ensure the extensive use of RFID for Internet of Things. In a few years, as RFID tags become smaller and smaller they will eventually reach the size of a nanoparticle and will subsequently become airborne, thus covering vast amounts of land and objects, including people. With this in mind these connected devices will sense every part of the environment around us and transmit their data in real time to form part of an intelligent system or Smart Grid, that can support and co-ordinate numerous tasks, to ensure they flow efficiently and automate everyday life [12].

4.2 NFC

Near field communication (NFC) is a wireless communication technology that enables communication between devices that are in close proximity to each other. Typically, it uses a set of communication protocols that work when the devices are touching or almost touching (within 10 cm from each other). NFC allows transmission of small packets of data between smart phones and the other NFC enabled devices. NFC devices can play one of the two roles of "initiator" (polling device) and "target" (listening device). The initiator initiates the communication and the target responds to the requests of the initiator. Basically, near field communication has been developed from the concept of RFID itself with few discrepancies. Near field communication (NFC) is an offshoot of RFID and shares many physical properties with RFID; the two technologies enable one way communication, and employ radio signals for different types of tracking and tagging purposes [13]. This technology is highly energy efficient as the power required by the tag to perform cryptographic operations is derived from the radiative near field.

NFC devices support three modes of operation (emulation, reader/writer, P2P), each one providing different functionality of its own. The NFC card emulation mode serves the function of making the device emulate credit cards or smart cards, NFC reader/writer mode makes it possible for the device to read or write data and Peer to Peer (P2P) mode allows data exchange between connected devices. NFC standards cover communications protocols and data exchange formats and are based on existing radio-frequency identification (RFID) standards including ISO/IEC 14443and FeliCa [14].

1) *NFC Reader/Writer Mode:* In the Reader/Writer mode, the NFC-enabled mobile device initiates the communication and it can read/write information in the target NFC tag such as a tag embedded in a smart poster or display it is connected to. A secure area is not required for the reader/writer mode. The RF

interface in the reader/writer mode follows ISO/IEC 14443 Type A and Type B.

2) *Peer to Peer Mode (P2P):* Peer to peer mode is a very useful feature of NFC as it creates a wireless virtual communication channel between two active NFC devices. The exchange of data takes place through this established channel in the half-duplex manner. Any kind of data such photos, media or visiting cards can be shared between the connected devices in this mode. The device which initiates the communication is the initiator and the receiver is the target. Data rate can reach a maximum of 424kbps.

3) *NFC Card Emulation Mode:* In the emulation mode, the active NFC-enabled mobile device emulates or imitates a smart card. Either an NFC enabled mobile phone emulates an ISO 14443 smart card or a smart card chip integrated in a mobile phone is connected to the antenna of the NFC module [15]. This mode allows users to make transactions like payment or ticketing.

TABLE V
DESCRIPTION of OPERATING MODES OF NFC[16]

Reader/Writer mode	**Peer-to-Peer mode**	**Card Emulation mode**
1. Increases mobility 2. Decreases physical effort 3. Ability to be adapted n many scenarios 4. Easy to implement	1. Easy data exchange 2. Device pairing	1. Physical object elimination 2. Access Control

With these modes, it is possible to establish two-way communication using NFC tags, which is its added advantage over RFID tags. Due to its three modes, the usability of NFC can be extended to numerous applications from a wide range of sectors like NFC Shopping (Reader/writer mode), NFC Gossiping (Peer-to-Peer mode) and NFC Ticketing (Card Emulation mode). In addition, NFC tags can simultaneously transmit and receive signals making full duplex communication possible. Owing to the short range, the connections are quite secure and less prone to interference which makes NFC perfect for making transactions, etc. It puts a limitation in terms of degree of closeness to the device on the attackers attempting to cause intrusions.

Smart phones can be embedded with NFC tags which can be used for cashless payments, and as bus pass, train tickets etc. Thanks to the P2P mode, NFC enabled devices and tags can be used instead of the keys or passwords. In some years NFC can replace all the identification badges and keys. Every user will have a unique tag which will enable the user to get access for any service. Using NFC in healthcare sector would make it easier for the patients to do their periodic check-ups or renew prescriptions or pay for the services rendered, all just by using a smart phone. The NFC technology is seen as the future of retail experience. NFC being much more secure than barcodes, will change the way we carry out our transactions and check outs. With connection time lesser than 0.1second, the speed of these transactions will also increase dramatically. NFC chips are small and lighter in weight than RFID tags. Hence they could eventually be integrated into movie posters, flyers or even on advertisement. NFC enabled movie posters or advertisements can be accessed with smart phones which will beam up the relevant information about the product. When compared to Bluetooth technology NFC has lower data rates but it doesn't require pairing as does Bluetooth, thus further ensuring faster connectivity. This is a very important factor to consider for its implementation in IoT networks as higher connection speeds mean lower latency and better performance.

As it seems, the role of NFC-enabled devices in future IoT networks will be crucial. Although it looks promising, currently the NFC technology is in its nascent state with a tremendous potential. Security threats like eavesdropping, data corruption, data modification, data insertion etc. are very challenging to tackle. To our advantage, it is possible in NFC to keep a continuous watch on the near RF field for any attacks. Any intrusion is hence possible to detect. NFC-SEC and NFC-SEC-01 are the security protocols which can be used to ensure the security of data in Peer-to-Peer mode. Breaches like data modification and eavesdropping can be overcome by establishing a secure channel over NFC using these NFC-SEC protocols. With further improvements in the efficiency and security provisions of this technology, large scale implementation will be possible. Advancements in the NFC technology will bring us a step closer to the realization of full-fledged smart environments.

5 RFID AND NFC

In the process of RFID items are identified using radio waves and NFC is a specialized subset within the family of RFID technology. Specifically, NFC is a branch of High-Frequency (HF) RFID, and both operate at the 13.56 MHz frequency. NFC is a secure form of data exchange, and an NFC device is capable of being both an NFC reader and an NFC tag which is not the case in the RFID. This peer to peer communication is a unique feature of the NFC. This ability has made NFC a popular choice for cashless payments, a key driver in the decision by companies in the mobile industry to include NFC in smart phones. Also, NFC smart phones pass along data packets from one phone to the other by tapping the two devices together, which turns sharing data such as documents or images into a simple task. On the other hand, the application of RFID is prevalent in almost all walks of life from medical sciences, animal husbandry, library, travel, agriculture to retail, consumer goods counting and tracking. It can be applied to Attendance system in educational institutions and

other work places in bank lockers for secured access, ware houses and storage places where lot inventory movement is expected. It is therefore evident that NFC and RFID are designed to achieve fundamentally different set of features. The close proximity requirement of the NFC tags can be thought of as a feature of NFC and not a limitation. NFC has successfully addressed the security and privacy concerns which are common in RFID technology. When used together in IoT, both contribute a separate set of functionalities, and this perfectly caters to the dream of an omnipresent network of things. Therefore, as both these technologies develop to become more efficient and foolproof, feasibility of IoT will be assured.

6 Future Scope

The future of RFID relies on the elimination of the problems which we are currently facing. To make RFID sustainable and useful for a wide range of applications there is a need of standardization. Currently use of RFID system in Internet of Things is vendor specific and for the past few years efforts are being made to create a platform for worldwide standards and interoperability. To replace the current tracking goods system (Barcode tracking) completely, RFID has to come up with the lower product cost solutions. Also RFID manufacturers are taking efforts towards making tag reading more secure and authorized. Lack of security will hinder the use of RFID in the IoT sector. Hence active smart tags are the future of the RFID technology where tags can also encrypt the information so that only intended reader can understand and process the data.[17]

Although RFID might seem to cater to almost all of the functions to make smart environments possible, the scope of NFC extends beyond it to achieve a different set of goals for the Internet of Things. The technological advancements in the NFC are still in its primitive stage and it will take few years before we see the complete potential of NFC in IoT, but it will undoubtedly play a crucial role in the development of the technological solutions in the sector. The main challenge of the NFC is to establish compatibility with other devices. NFC being a relatively new technology, overcoming the challenge of device compatibility is going to play a vital role in expansion of the consumer base of IoT. Also malware interception attacks make NFC technology vulnerable. Hence antivirus software and specific operating system architecture which can sustain such malware attacks is under developmental stage.[18] To avoid security breaches in the future, researchers are working on the secure data transmission and reception channels. Elimination of these drawbacks in the constituent technologies is necessary in order to make IoT possible. Reliability is another necessary factor for any emerging technology. Rest of the developments will be redundant if the technology is not reliable enough in terms of security and privacy. Hence before the large scale employment of the IoT technology, extensive and confined research would be the prime area where its future would be decided.

7 Conclusion

Future lies in automation and smart environments, and Internet of Things is going to play a vital role in achieving this. It is still in the experimental stage, and is rapidly transforming everyday physical objects into smart and more intuitive appliances. Right from refrigerators in our kitchens to the smart payment options, IoT is bringing more and more things into digital world every day, making it an industry with huge potential in near future. In this paper we focused on two important M2M communication technologies for IoT i.e. RFID and NFC and pointed out the possibility of their contributions in realizing Internet of Things. These technologies are nothing but two key components among many others which have the capability to boost the Internet of the Things and impact the future of Machine to Machine communication strategies.

References

[1] Andrea Zanella, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, and Michele Zorzi, "Internet of Things for Smart Cities" IEEE Internet of Things Journal, Volume. 1, No. 1, February 2014 .

[2] Yang, Dehuai (Ed.)," Informatics in Control, Automation and Robotics, Volume 2" Lecture notes in Electrical Engineering 133, Springer.

[3] Dr. Ovidiu Vermesan, Dr. Peter Friess, "Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems" River Publishers, 9000 Aalborg, Denmark.

[4] White Paper "What the Internet of Things (IoT) Needs to Become a Reality", arm.com / freescale.com.

[5] White Paper, Jim Chase "The Evolution of the Internet of Things", Texas Instruments, September 2013.

[6] Friedemann Mattern, Christian Floerkemeier, "From the Internet of Computers to the Internet of Things", Distributed Systems Group, Institute for Pervasive Computing, ETH Zurich.

[7] Stephen A. Weis, "RFID (Radio Frequency Identification): Principles and Applications", MIT CSAIL.

[8] EPCglobal. (2006). Webpage. Available at: http://www.epcglobalinc.org. (Last Accessed: March 11, 2006.).

[9] "Ants' home search habit uncovered". BBC News. 2009-04-22. Retrieved 2013-09-03

[10] "Hitachi's RFID powder freaks us the heck out". Engadget. Retrieved 2010-04-24

[11] "RFID Forecasts, Players and Opportunities in 2014-2024". IDTechEx

[12] Simon Sothcott, "What is RFID? - 10 Examples of RFID Applications" , Wednesday, 2 November 2011, http://www.simonsothcott.com

[13] The Sine Wave Blog, "RFID vs NFC: Their role in the Internet of Things", http://www.sine-wave.com/blog/nfc, November 21, 2013.

[14] Electronista Article: New NFC spec lets two phones swap messages, October 2011

[15] Ms. Bhoomika Gupta,"Near Field Communication and Application", November 2013

[16] B. Ozdenizci, M. N. Aydin, V. Coskun, K. Ok, "NFC Research Framework: A Literature Review and Future Research Directions", Proc. 14th IBIMA International Business Information Management Conf., Istanbul, TURKEY, 2010, pp. 2672-2685.

[17] Roy Want, "An Introduction to RFID Technology", IEEE Pervasive Computing, vol. 5, no. 1, pp. 25-33, Jan.-Mar. 2006

[18] Vibhor Sharma, Preeti Gusain, Prashant Kumar, "Near Field Communication", Conferences on Advances in Communication and Control System 2013 (CAC2S 2013).