TNC Transactions on Networks and Communications
SOCIETY FOR SCIENCE AND EDUCATION UNITED KINGDOM
VOLUME 3, ISSUE 3
ISSN: 2054 - 7420

Radio Frequency Identification Upon Near Field Communication and Far Field Communication For Next Generation Wireless Network Infrastructures

Gowher Mushtaq, Shashank Singh, Neeraj Kumar Tiwari, Seemab Rasheed, Yogesh pal
gowhermushtaq@ymail.com

ABSTRACT

The electromagnetic field that outlines the RFID antenna can be divided up into two portions – Near-field and Far-field. Near Field Communication (NFC) and Far-Field communication (FFC) both are the most emerging wireless short-range communication technologies, both are based on existing standards of the Radio Frequency Identification (RFID) network framework. In collaboration with NFC-efficient next generation smartphones it authorizes automatic application frameworks for contact less connections, in different exceptional utilities for future generation smartphone payment and over-the air ticketing. The principle aim of current study is to explain basic characteristics and benefits of the wireless short- range technologies like (RFID, NFC, and FFC) and analogy between them to classify modes of operation and to present various illustrations. NFC mechanism, applications and FFC with possible future or Next Generation scenarios will be analyzed. Finally, this study provides the fundamental security concerns; challenges and present conflicts will be investigated in order to achieve the efficiency in Next Generation Network Infrastructures.

Keywords: Electromagnetic Field, RFID, NFC, FFC, Smartphones, Next Generation

1 Introduction

According to the study work of Roy Want in [1], “Radio Frequency Identification Technology (RFID) has been developed from complexity into main stream applications that let us help to rate the manipulating of assembled figures and stocks facts”. Accordingly, Bar code which is probably the best performer in transmitting sequence of productions and organizational warehouses in the future generation network infrastructures. However, RFID is exchanging bar code technology and be entertained by one of the crucial advantage of being independent of line of sight problems and scanning the objects from a distance. It anticipates the skeleton of amplified visibility, updated tabulation management and decreased labor levels. According to the latest information standards, Wal-Mart has been one of the leaders in the large scale adoption of RFID technology [1]. RFID tags have a memory capacity of 16 - 64 Kbytes which is far more than the barcodes (1 - 100 bytes) [1] and can store additional data such as manufacturer name and product specifications.

The initial step for the development of RFID was during World War II, when the British manipulates it to identify whether planes belonged to “friend or enemy”. Some technical problems resulted in the gunning down of allied planes and since then the use of RFID was limited to Defense and armed forces industries due to the cost factors. New advancements in science and technology have enabled usage in commercial applications. Large institutions, such as the US Department of Defense, have since implemented RFID which is now spreading to other organizations and Multi-National companies [1].

DOI: 10.14738/tnc.33.1167
Publication Date: 9th May 2015
URL: http://dx.doi.org/10.14738/tnc.33.1167

Wal-Mart is the world's second biggest user of RFID and investing significant resources to develop its highly efficient applications. RFID technology operates at multiple frequencies counting low, high and ultra-high. The frequency that is being carried out discovers the distance in which RFID tags can be measured, how many tags can be interpreted at one time, how fast these tags are calculated, and how can application framework will influence its performance.

When making a choice between two technologies, it is significant to acknowledge their separate program propriety, implementation abilities, intensities, and deficiency. By surveying the different utilizing principles and future habitat affects, we should make a literate conclusion advance to implementing any path and explore technology. One more satisfaction, when deciding the proper frequency for a communicating application is the quantity of electromagnetic interference (EMI) and sensitivity to exterior programmer components i.e. water, metal, Muscularity, evaporation, or any other data influence, inversion, etc. Within the last few years a communicative technique has appear to emerge integrating computational cognition into different kinds of objects of our day to day life and permitting we people to constantly connect with those objects. The proposal is to positively connect virtual information to objects of the material world and therefore providing global computing. Comparable to the abstraction of network universality is the term 'Internet of Things' introducing to objects of daily use being verifiable, measurable and even virtually connected via an internet-like framework [2].

A leading designer for this perception is the technology of Near Field Communication (NFC) that provides the possibility of linking virtual information between physical devices via adjacency. Virtually all object or place can be assembled with a NFC tag and thus provide proximate identification and useful related information to a nearby user of a smart device, like a tablet computer or a smart phone [2].

The intention of this study is to summarize opportunities provided by Radio Frequency Identification combining the technology of Near Field Communication and Far Field Communication with the capabilities of modern smartphones. It will point out recent trends and present application scenarios, but also address challenges and obstacles that might occur when trying to make NFC suitable for the mass market.

First, it will be necessary to provide a basic technical understanding of Near Field Communication. The first chapter will thus roughly explain the functionality of NFC and its underlying technique of Radio Frequency Identification (RFID). Its characteristics will be described and necessary hardware components and different modes of operation will be specified. Furthermore, examples for mobile ticketing will also be discussed as well as possible applications for medical assistance and for other market segments. The final part of this paper will deal with potential security issues and other challenges mostly related to present conflicts due to clashing interest of different groups of stakeholders. Addressing this topic is essential for eventually providing an outlook for the future development and estimation for the expected prospect of success in the context of RFID with respect to Near Field Communication and Far Field Communication.

2 Related work

The NFC technology was launched in 2004, when it was regulated by NFC forum. NFC forum act as an authority to define NFC standards and specifications. It is also responsible for technology's further

improvement. NFC standards are defined in ISO 18092 and in its counterpart ECMA-340 standard. The technology of NFC and FFC has been yielded from RFID (Radio frequency Identification) and is also consistent with this. However, NFC technology is being observed RFID‟s apparent and RFID is its scion. The aspects drafted for RFID technology i.e. RFID tags or devices are emerged with standard ISO 14443 and are also acceptable to function with NFC technology. Besides, NFC devices are also well matched with RFID tags from MIFARE and FeliCa brands, developed by Philips and Sony respectively [3]. In this bodywork, the survived literature has been classified into theoretical fields and applications. The imaginary areas include security, technology, organization, and privacy.

RFID tags fall into two categories, active tags, which consists an internal energy authority, and passive tags, which gathers energy from the wave of an external reader. A passive tag consists of a microchip enclosed by a printed antenna and some type of encapsulation, plastic laminates with viscous that can be connected to a product or a small glass bottle for convention. The tag reader powers and communicates with passive tags. The tag's antenna organizes the process of ID transfer and energy capture. A tag's chip frequently occupies data to analyze a sole product, the product model and manufacturer.

NFC is a short-range wireless communication technology that is placed on authorized and sophisticated standards in the field of RFID and smart cards. RFID, which has been made known in the 1970s, recognizes robotic description and data transfer via electromagnetic radio signals consistently by means of an active reader that is connected to a source of energy and a passive electronic tag that is a transponder receiving its power from the reader by magnetic induction.

3 Research Methodology

The fundamental motive of this study is to explain basic characteristics and benefits of the underlying technologies (RFID, NFC, and FFC) and the comparison between them, to classify modes of operation and to present various illustrations. NFC applications, mechanism and FFC with possible future or Next Generation scenarios will be analyzed in this paper. Finally this study provides the fundamental security concerns; challenges and present conflicts that will be investigated in order to achieve the efficiency in Next Generation Network Infrastructures with respect to Radio Frequency Identification.

3.1 RFID (Radio Frequency Identification)

Radio Frequency Identification (RFID) is a form of automatic identification technology (auto ID). Auto ID is characterized by data forms that are machine readable. Other classification of Auto ID contain electronic article surveillance (EAS) safety tags, bar codes, magnetic stripes, optical character recognition, optical character group (OCG) etc. These technologies can be additionally identified by those that need contact in order to be read (magnetic stripes), and those that do not (such as, bar codes, EAS, OCG, RFID). RFID differs from bar codes and most other contactless auto ID data forms in that the data can be read without a direct line of sight to the reader. Additionally, read intervals can be comparatively high (feet versus inches). Utilizing RFID measures that:

- Compact human embarrassment is needed for the proper information or data improvement.
- Improvement can be fast-moving.
- With the perfectly installed and influenced system, data represented through RFID is more authentic and obtained at lower costs.

This high-level standard of automation makes RFID self-confident to be an auto ID technology that could change the way in which information is collected and utilized.

Presently, RFID is utilized in various applications, oscillating from computerized installments for tracking goods during the supply chain. The utilization of RFID technology in closed-loop systems is as powerful as applications for chasing goods. In 2008, the quantity of RFID chips used in different closed-loop, mass movement tickets and cards was about balanced to those utilized in open- supply chain goods recording. A Radio Frequency Identification (RFID) system consists of readers (also called interrogators) and tags (or transponders). A classic system has a few readers, either static or mobile, and various tags, which are connected to objects, such as bottles, platforms, cartons, etc. A reader broadcasts with the tags in its wireless domain and gathers information about the objects to which tags are connected. Depending upon their working theory, tags are categorized into three headings:

- Passive,
- Semi-Passive, and
- Active.

A passive tag is the least sophisticated and consequently the cheapest. It has got no interior energy maternity but in order get better transmission results passive tag uses the electromagnetic field (EM) transmitted by a reader to power its interior router. It acts on “back-scattering” not on a transmitter to transmit data reverse to the reader. A semi-passive tag has got its own energy source but it has got no transmitter and also utilizes back-scattering. While as in comparison to both of the two tags, an active tag has both internal power supply and an on-tag transmitter.

A simple Example of Closed Loop System:

An example of a closed loop system is the disaster expulsion system for the humor of Texas. The Texas regional jurisdictions along with National companion, provides consolation to common people that are requesting for the help to move out from the awaiting disaster (cyclones are the common example). The efforts that are attached with the disaster were historically efficient, but planning for understanding the evacuation progress, shelter, getting information’s about the individual with their location and being able to respond to concerned relatives required great effort including calling many shelters sites and hospitals to locate family members.

In 2008, Texas put into effect a spontaneous RFID-based Special Needs Evacuation Tracking System (SNETS), developed by LLC, Radiant RFID, to help manage the overall evacuation. Almost every person who needs aid can choose to wear the RFID wristband. The particular wireless wristband is made up of a unique number, bar code and electronic code that associate to the person’s private data in a secure database. The wristband is read at expulsion bus conversion points, boarding sites, and final shelter locations. People like friends; relatives etc. can contact a 211 or 800 number which is printed on the band and request that the displaced person can contact them. State officials then locate the displaced person in the SNETS database, and notify the migrant in the inquiry. The wristband interference system certifies the messages delivered to the right expulsion location’s electronic message center, and gets permission for recovery communications. The particular system does not acknowledge the displaced person’s location (only that person which is displaced from her/his location can expose his/her position, through a message).

With the speed and reliability of RFID tag reads, this system is effective during the urgent pace of evacuating large numbers of people. More than 40 thousand wristbands were issued and deployed in 2008 for Hurricanes Ike and Gustav in Texas.

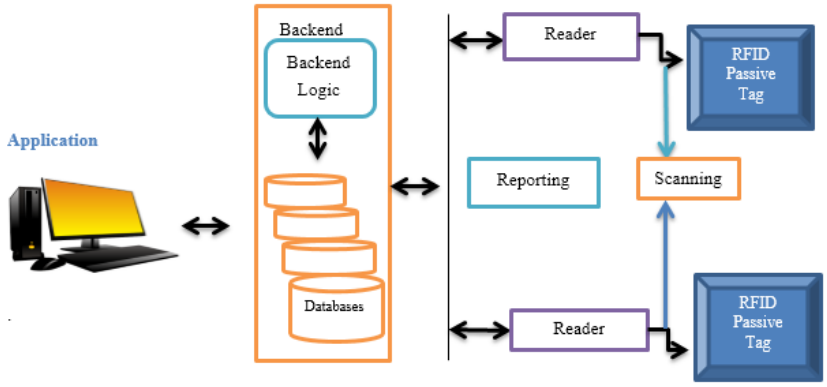

Figure 1: A simplified RFID System

In RFID, reader and some other particular tags in general are having a little use. The healing of a sequence number does not provide much information to the user and nor does it help to keep record of items in a management group. The absolute energy of RFID arrives in consolidation with a tail end that stores extra information like confession about the products, when and where a positive tag was investigated. Furthermore, the RFID system has been described through structure as explained in figure 1. RFID readers firstly, scan tags and then transfer the information to the backend. The backend in normal form consists of a database and a well-defined application interface. When the backend gathers some additional source or what we can say information that particular information is stored in the database for further processing, and if required it implements some computation on associated disciplines. The application brings back the data or information from the backend. Through various scenarios, the application is assembled with the reader itself. An example of this particular scenario is the consistent point in a shopping center (Note that the specific example uses barcodes rather than RFID tags after all they are highly accepted, in spite of, the system would act in absolutely the same manner if tags were utilized). The application uses the copied identifier to take care of the current cost when RFID reader scans the barcode. In inclusion to that, the application backend also transfers premium information for certified commodities. The backend also reduces the sum of feasible commodities of that type and alerts the manager if the quantity falls below a sure verge.

3.2 RFID classification

The classification of Radio Frequency Identification is showing below through a diagram

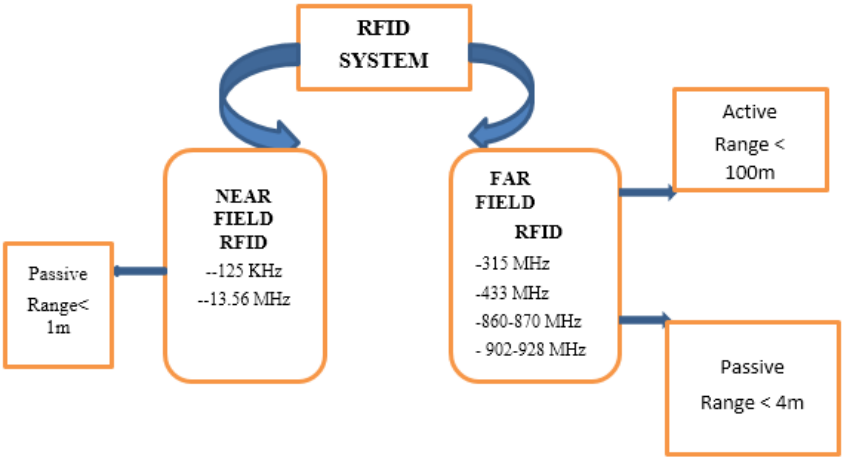

Figure 2. Showing the Classification of RFID

3.3 Brief History

The concept of communication using reflected radio energy is quite old and dates back to the origin of radar technology. Many developments in the early 20th century applied radio back-scatter. For example, the Identify-Friend or Foe (IFF) transponder developed by British was used by the allies in World War II for identification of friendly aircraft. It relied on passive radar reflectors, tuned to the home radar frequency, which made a friendly aircraft much brighter to home radar than an enemy aircraft.

Among the earliest and significant works related to RFID is the continuous time modulation of reflected signals, published by Stockman in October 1948 [5]. While he was working at the Air Materiel Command in Massachusetts, he launched a device and designed it in the way which modulated human voice on reflected light signals. The decagons of the 1960s and 1970s were marked by the research community's interest in RFID. An early breakthrough of this period was a passive RFID transponder developed and patented by Richardson in July 1963. The device could couple and rectify energy from an interrogator's EM field and transmit signals at a harmonic of the received frequency. Later in the decade, Vinding developed a simple and inexpensive interrogator-transponder system based on inductive coupling, which was granted a U.S. patent in January 1967[5]. The transponder used repetitive tuning or loading of its antenna circuit at a rate characteristic of the particular transponder under interrogation. Koelle, Depp and Freyman, while at Los Alamos Scientific Laboratory (LASL) in northern New Mexico, introduced the novel concept of transponder antenna load modulation as a simple and effective way for backscatter modulation in August 1975.

The first commercial application of RFID — Electronic Article Surveillance, was introduced by associations such as Sensormatic, Kongo, and Checkpoint in the late 1960s. Commercialization picked up in the 1980s and 1990s with varying interest in different parts of the universe. Fundamental interests in the United States constitute office connection and transportation, during European countries were interested in short-range systems for tracking animals, industrial and business applications and electronic toll-collection. The first RFID-based toll-collection system became practical in Ålesund, Norway in October 1987. The development in commercial use of RFID, the organization of RFID suggests a requirement for assumptions, which assist to numerous standardization activities in the 1990s. Most of these were conducted by the International Electro-technical Commission (IEC) and International Standards Organization (ISO).

ISO, an international organization upon which 157 countries belong, develops industry-wide standards in a series of greens. Accordingly, IEC is likewise a global organization; however it concentrates on standards for electronics, electrical, and related technologies. Basic similarity concerns are in animal tracking (ISO-11784 and ISO-11785) and contactless proximity cards (ISO-14443) applications. The 1990s saw the acceptance of RFID as an important enabler in supply chain management, which spurred a further series of standardization activities.

A milestone came in 1996 with the standardization of RFID as a data carrier by the Article Number Association (ANA) and European Article Numbering (EAN) groups. In 1999, EAN International, and the Uniform Code Council (UCC) of the United States, now both known as GS1, adopted a UHF frequency band for RFID and established the Auto-ID Center at the Massachusetts.

Only recently have advances in silicon technology made RFID tags cheap and reliable. Thus, the first decade of the 21st century sees the world moving toward the technology's widespread and large-scale adoption. A major landmark was the announcement by Wal-Mart Inc., in the USA, to authorize RFID for its suppliers in "the near future," at the Retail Systems Conference in June 2003 in Chicago. This was followed by the release of the first EPC global standard in January 2005. Till date more than 1000 Wal-Mart locations have already implemented EPC RFID standard. This organization was charged with developing a global RFID standard for product labeling called the Electronic Product Code (EPC). The Auto-ID Center later evolved into Auto-ID Labs and EPC global Inc. The latter is a nonprofit organization, set up by UCC and EAN International, pursuing the commercialization of EPC technology.

3.4 Types of Tags in RFID

RFID tags fall into two categories, active tags, which contain an internal power source, and passive tags, which obtain power from the signal of an external reader. Because of their lower price and smaller size, passive tags are more commonly used then active tags for retail purposes. A passive tag consists of a microchip surrounded by a printed antenna and some form of encapsulation, plastic laminates with adhesive that can be attached to a product or a small glass vial for implantation. The tag reader powers and communicates with passive tags. The tag's antenna conducts the process of energy capture and ID transfer. A tag's chip typically holds data to identify an individual product, the product model and manufacturer. The difference between active and passive tags of RFID is given below in a table:

Table 1. RFID Active tag vs. Passive tag.

Active Tags	Passive Tags
Transmit a stronger Signal	Transmit a weaker Signal
Have a longer "read" range, can exceed 100 meters, Depending on antenna size	Read distance ranges of 10 cm. to a few meters
Operate at higher frequencies-commonly 455 MHz, 2.45 GHz, or 5.8 GHz	Typical operating frequencies- 128 KHz, 13.6 MHz, 915 MHz, or 2.45 GHz
Expire after battery power runs out	Operate until damaged or discarded
Cost a few dollars per tag	Cost 7.9 cents per tag when purchased in quantities of 1 million (as of May 2006)
Size is typically slightly larger than a deck of playing cards	Can be as small as a grain of rice

Without a power supply of their own, passive RFID tags depend upon the electromagnetic field of the reader. The paired power is improved and the electromagnetism is amplified to power up interior circuits. A multi-stage Greinacher half-wave magnetism or a derivative is normally used for this purpose. There are two different coupling techniques, near and far fields, which are used by passive tags.

3.4.1 Near Field Coupling

The EM field in the near-field area is sensitive in nature-the electric and the magnetic fields are rectangular and virtual-static. It mostly depends upon the type of antenna; one field (such as the electric field for a dipole or magnetic field for a coil) controls the other field. Most near-field tags rely on the magnetic field through inductive coupling to the coil in the tag. This mechanism is generally

based upon Faraday's principle of magnetic induction. A current flowing through the coil of a reader produces a magnetic field around it. This field causes a tag's coil in the vicinity to generate a small current. Communication between a reader and a tag is through a mechanism called load modulation. Any variation of the current in a tag's coil causes a small current variation in a reader's coil due to the mutual inductance between the two, and the variation is detected by reader. A tag varies the current by changing the load on its antenna coil, and hence the mechanism is called load modulation. Because of its simplicity, inductive coupling was initially adopted for passive RFID systems. Depending upon the application, near-field tags come in many form factors as shown in figure 3

The boundary between near-field and far-field regions is inversely proportional to frequency and approximately equal to c/2f, where c is the speed of light [3]. Therefore, only low carrier frequencies are used in near-field coupling tags; the two most common are 128 kHz (LF) and 13.56 MHz (HF). For example, the boundary distances are 372 m1 for 128 kHz and 3.5 m for 13.56 MHz One problem with use of low frequencies is that a large antenna coil is required. Also, the power of magnetic field of a magnetic dipole loop drops as 1/r6 in the near-field region, where r is the distance between a reader and a tag. Another downside is the low bandwidth and, hence, the low data rate

3.4.2 Far-Field Coupling

The EM field in the far-field region is radioactive in nature. Coupling here captures EM energy at a tag's antenna as a potential difference. Part of the energy incident on a tag's antenna is reflected back due to an impedance mismatch between the antenna and the load circuit. Changing the mismatch or loading on the antenna can vary the amount of reflected energy, a technique called backscattering.

Far-field coupling is commonly employed for long-range (5–20 m) RFID, and, in contrast to near-field, there is no restriction on the field boundary for far-field RFID. The Several emerging technologies in the UHF and LF bands try to exploit advantages of both near-field and far-field tags. UHF proponents are promoting near-field UHF tags for label tagging, which has been the sole domain of HF near-field tags. The advantage of using UHF here is the low tag cost, resulting from small antenna size. RuBee, a relatively new active RFID technology, operates in the LF band and employs long-wave magnetic signaling. It can achieve a read range of 30 m. Long-wave magnetic signaling has a great advantage: it is highly resistant to performance degradation near metal objects and water, a serious problem for UHF and Microwave far-field RFID.

RFID NFC anti-metal tag on mobile phone

Table 2. RFID/NFC anti-metal tag on smart phones

Antenna Dimension	**76X45mm (±0.2 mm)**
Final dimension	85X54mm (±0.5mm)
Antenna skip distance	88.6±0.4 mm
Antenna margin	7.0±1.0 mm
Width of the Tape	59.0±1.0 mm
Antenna number /square meter of typesetting	176 pcs

Table 3. RFID product features

Features of RFID (NFC, FFC) showing the various attributes with their standards and characteristic's:

Substrate Material	**Polyester Film（PET）**
The Antenna Material	Aluminum Etching
Surface Material	Wave-absorbing Material +Surface Label Printing
Characteristics	the Flexible Label
Product Attribute used in the metal surface	Waterproof, acid proof, alkali proof, collision and can be used outdoors, can be well effectively prevent metal of the radio frequency signal interference
Operating Frequency	13.0MHZ ～14.5MHZ
Supported Protocol	ISO/IEC14443-A
Chip IC	FM11RF08 (other compatible chips option)
MEMORY & SECURITY	1024bit X 8
Operating Mode	Inventory Read or Write
Reading Distance	≥1CM（Reader：Desktop Reader IVF-RH11）
Programming Cycle	100,000 cycles

Environmental Parameter of RFID

Table 4. Environmental Parameters.

Operating Temperature	-25℃～75℃
Storage Temperature	0℃～25℃

Table 5. Packing in RFID.

Packing in RFID

Core Diameter	76.2mm (3inch)
Volume Number	2000～5000PCS (According to Actual Demand)
The Roll Direction	the Surface or Printing Facing out (up)
Packing Material	Antistatic PE + Bubble Pad + Antistatic Bag + Paper Carton/Box

3.5 RFID Deployment and Concerns

Since RFID was first introduced in World War II to identify aircraft, the technology has improved as it has been implemented in a broad variety of uses, including identifying livestock and pets; shipping containers; managing vehicle fleets; increasing highway throughput; speeding up transactions at the point of sale; gaining entrance to buildings; real time asset tracking and mass transit ticketing. In the wake of 9/11, RFID is efficiently being utilized to boost the reliability of separate designs of recognition, without producing longer ID reliability verification wait times. Many collections of RFID exist in our daily life. Each requires to be verified separately. The technical and economic conclusions between the different collections explain that decisions in respect to the choice of users, including solution providers and other system integrators, hold the key to successful implementation of the future technology.

RFID is not yet a plug-and-play product technology. A few workers will take the "one-solution-fits-all" terminology, which leads to various difficulties and obstacles. Although, when the best design is preferred, it may require a self-design particular application to attain the excellent performance. The

settlements mostly require to be classified. For example, can the outstanding performance of a more costly self-design dominate the economics of employing an off-the-shelf design?

RFID under performs in some particular applications because of a non-optimized solution technique. The typical understanding of RFID, its collections, and self-design tools are important when calculating its future utilization in an auto ID program. Too often, the underlying engineering and physics are not understood, minimal training is provided, and expectations are unrealistic. Consumer privacy and data security concerns are heightened by the longer read distances capable with RFID. The technology creates an opportunity for unsolicited RFID tag data modifications (reads/writes), and/or reads of which the tag carrier is unaware. This concern is somehow unique to RFID forms of auto ID. Some collections of RFID have built-in security protocols to ensure only authorized readers talk with only authentic tags. Most of these secure collections also have technology design standards that limit data transaction distances to fingerbreadth, vs. feet, that takes care of data to reduce the threat from hackers. Another visible feature of security is whether to transfer particular ID data on the tag (and authorize data security to the reader framework), or having a specific RFID tag containing a "license plate" that connects to the real data, adhered in a secure master data base. This conclusion is mostly built on one application in a particular time. Measures and governances for RFID technology rest with the industry to which the wireless technology is being enforced.

With a limited inspiration, sustained by sci-fi computation, and the scarcity of brutal study, another concern hides. Someone who adopts the emergency of RFID-tagged commodities do that with practical clerical intensity. The concern of privately or secretly being tracked is perfectly impractical, but security issues are expanding as RFID is being employed in more private id applications, like passports, credit cards and retail goods tagging.

Another concern is the security of proprietary data. How much does one company want to reveal to a competitor to gain efficiencies? That dilemma is of special concern in extremely aggressive industries and companies, for example, pharmaceuticals. Sharing data in an open supply chain means the manufacturer may have to share its pricing throughout the supply chain, including its competitors. Databases supporting open supply chain networks must be built with the understanding that some data must remain protected.

The ultimate issue is the loss of global RF management regarding reader power, acceptable frequencies, and sideband spectrums levels. Likely, we know that our frugality is global, still there is a scarcity of typical settlements, and more efficiently the connected system achievement generates extra-ordinary changes, engineering expense-effective solutions for the Universal open supply series is challenging and complicated. This scarcity of Universal standardization and regulation prevents the approval of RFID as an open supply series mechanism.

The terminology explains that RFID technology has the power to impact the supply series, both positively and negatively. The potential to transfer information digitally, during the entire life of services and goods, will generate an enormous transformation in the global supply series operations and helps in providing authentic goods reach their destination. That a product can bisect the whole shipping and distribution network easily does not imply that the means to manage it will be simple. This is first phase of utilizing the technology globally.

3.6 Frequency Bands in RFID

RFID tags are divided into three regions with respect to frequency:

- Low frequency (30 - 500kHz, LF)
- High frequency (10 - 15MHz,HF)
- Ultra high frequency (5.8GHz, 2.4 - 2.5GHz, 850 – 950MHz, , UHF)

Low frequency tags are inexpensive than any of the powerful frequency tags. These are secure and quick sufficient for some of the particular applications, although there is massive quantity of data available, a tag has to stay in a reader's spectrum and it will boost the duration. Another benefit is that low frequency tags are slight damaged by the existence of fluids or metal. The disadvantage of such type of tags is their limited reading spectrum. The most particular frequencies used for low frequency tags are 140 - 148.5 kHz and 125 - 134.2 kHz. Long frequency tags have higher transmission rates and ranges but also cost more than LF tags. Smart tags are the most global member of this group and they work at the frequency spectrum of 13.56MHz.

In comparison to various tags, UHF tags have the highest spectrum of all tags. The spectrum ranges from 3-6 meters for passive tags and 30+ meters for active tags. Apart from that the transmission rate of UHF tags is also very high, which permits to read a single tag in a real manner of time. This attribute is very crucial where tagged entities are moving with a high speed and remain only for a short time in a readers range. Also, UHF tags are more expensive than the native tags and are generally affected by fluids and metal. So, with the help of these excellent properties this is main reason that UHF tags are particularly useful in automated toll collection systems. Typical Frequencies are 950MHz (Japan), 868MHz (Europe), 915MHz (USA), and 2.45GHz. Frequencies for LF and HF tags are license exempt and can be utilized globally; however frequencies for UHF tags differ from Nation to Nation and needs the permission for communication.

3.7 Working of RFID

RFID is virtually the information which is transported by the radio waves. The future technology came into existence from the fields of radar and radio engineering. Magnetic or electromagnetic fields have been used for the data transfer between the RFID transponder and the reader and, in passive RFID collections, are also used to hand over the power supply to the RFID transponder.

The components of an RFID field are:

The transponder or "tag" is the data transporting component of an RFID system. RFID tag data space normally ranges from a few bits to several kilobytes. A tag generally having an electronic microchip and chip antennae designed to permit communications with a reader. In a "passive" system the tag is mechanized by pairing with the reader field. An active tag may be totally or partially mechanized through its own battery source. Tags may be designed to be read-only or to read and accept writes. Tags are typically clustered for the clear-cut application. Tags may be planted in a collection of materials, including plastic cards, paper cards, injection molded plastics (such as key fobs), and glass (for use in a bodies such as animal identification). The typical method used for sending data from the transponder back to the tag is backscatter, in which the frequency of the reflected wave correlates with the frequency of the transmission from the reader. The transponder, or 'tag', consists of:

1. A microchip. These are now in our day life as small as 0.4mm by 0.4mm. Size of the microchip is often a principal factor in its cost, since the smaller the chip, the greater the produce from a constructed cracker. The cracker is processed by being manipulated to final chip consistency,

speculated into separate chips, and further more knocked for fasten, wire, or flip chip connection to an antenna. The chips are basically factory-programmed with an ID number during their contact testing stage. This pre-programming allows the utilization of the separate chip number in later stages of testing.

2. A chip antenna, designed for either electromagnetic or magnetic fields. The antenna is originated on a typical substrate (e.g., PET). The antenna can be etched copper, wires, etched aluminum, or printed conductive silver ink, and a growing array of aluminum or copper antennae are being made with preservative processes, such as electroplating. The material of antenna does edict positive achievement characteristics, and a particular type may be more optimal in a given application. Wire antennae are often used in 125-134 kHz (lf) tags, as the high number of winding turns required at this frequency is easiest to achieve in a realistic footprint with small diameter wires.

The connection operation is used to secure the chip onto the antennae substrate and electrically connect the chip to the antennae. The chip bumping technique, antennae information, and connection operation must be engineered together. After chip connection, decorate is RFID-functional and is ready to be packaged. Once decorate is packaged into a label, paper ticket, plastic card, or other material, a final test is typically conducted on each unit, and non-conforming units are highlighted and sometimes completely removed. The testing also permits writing to be done to each chip with respect of a rare ID number. Programming of large data or object specific data, such as an electronic product code (EPC), is normally done near the end application (for example, with an RFID-enabled bar code printer systems). The reader typically consists of a radio frequency receiver and sometimes a transmitter, a control unit, and antennae to provide data retrieval or communication: It can be thought of as a digital communications system. The chips and reader can be arranged to be Read-Only or vice-versa. Also readers may also be arranged for the communication with the capability to transmit the received data to another destination (e.g., via RS 232). The reader is used to provide commands to the tag, timing pulses and data, as well as paired energy for passive tags. It also receives data from the tag and must decipher this data relative to ambient RF noise. Most readers are designed to operate at a single channel or frequency. There are some designs that can read multiple protocols at different frequencies, but single channel frequency readers rule the day.

Reader system sizes range from the large fixed reader systems (size similar to shoplifting gates used in retail stores and libraries) that have the highest energy (and thus the longest read distances), to the smaller mid powered readers, and even smaller handheld readers powered by batteries. A unique feature of RFID is the ability to have multiple tags in the read field simultaneously. The system design feature that allows this is referred to as anti-collision. Anti-collision protocols are now part of many RFID standards, so that any vendor's chip can work with any vendor's reader when both are designed per a common set of standards. Anti-collision performance varies from reading a few tags per second to hundreds per second, depending on the frequency, the standard, and the amount of data on the chip to be read.

The reader antenna is important to the RF operation of the reader. Reader antennae designs can be made to maximize read distance, requiring tighter tolerances for the tag-to-reader coupling orientation, or they can be designed to be more robust to the tag-to-reader coupling orientation, but sacrifice some read distance.

The Federal Communications Commission (FCC) regulates the frequency and reader system RF emissions. RFID is operated at a shared frequency band, so care must be taken to prevent cross interference of RF systems sharing the same frequency band. Software for RFID-derived data is typically designed to filter the large amounts of repetitive data capture inherent in many RFID systems. This filtered data is then used by application-specific host systems. Higher end readers may have data filtering capability designed in. The software may also act as a data verifier and require multiple tag reads at a given reader before accepting that tag as a legitimate. Table 6. Explaining a comparison study of various types of operational frequencies of RFID with respect to NFC and FFC.

Table 6. Summary of Operational Frequencies.

Frequency Ranges	**LF 125 KHz**	**HF 13.56 MHz**	**UHF 868-915MHz**	**Microwave 2.45 GHz & 5.8 GHz**
Typical Max Read Range (Passive Tags)	Shortest 1"12"	Short 2"24"	Medium 1'-10'	Longest 1'15'
Data Rate	Slower	Moderate	Fast	Faster
Applications	Access Control & Security Identifying widgets Through manufacturing processes or in harsh environments Ranch animal identification Employee IDs	Library books Laundry identification Access Control Employee IDs	Supply chain tracking Highway toll Tags	Highway toll Tags Identification of private vehicle fleets in/out of a yard or facility Asset tracking
Tag Power Source	Generally passive tags only, using inductive coupling	Generally passive tags only, using inductive or capacitive coupling	Active tags with integral battery or passive tags using capacitive storage, Efield coupling	Active tags with integral battery or passive tags using capacitive storage, Efield coupling
Ability to read Near metal or wet surfaces	Better	Moderate	Poor	Worse

3.8 Proposed Structure and Design of RFID System

As shown in the fig.4, the process begins when RFID tag comes in the range of the RFID reader then the reader transmits the signals to the tag. Then tag will modulate that carrier signal with the data present in it. Then this modulated signal will be received by the RFID reader.

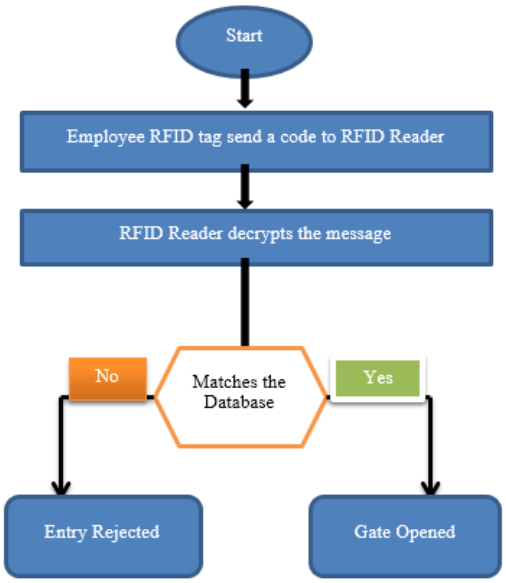

Figure. 4. Flow Chart Design of RFID based Security System.

The reader is having the RS232 interface so the data will be transferred from the transmitter (Tx) pin of reader to the 3rd pin i.e. transmitted data (TxD) pin of the RS232 port. Then the data is taken from TxD pin and is given to the 13th pin of the MAX 232 and output is taken from the 12th pin of MAX232 and is given as the input for the microcontroller. Here MAX232 will change standards from RS232 level to the TTL level standards. The input is given to the Rxd (P3^0) pin of 8051 microcontroller. In the microcontroller there will be code for the identification of the person and output which is either low (0) or high.

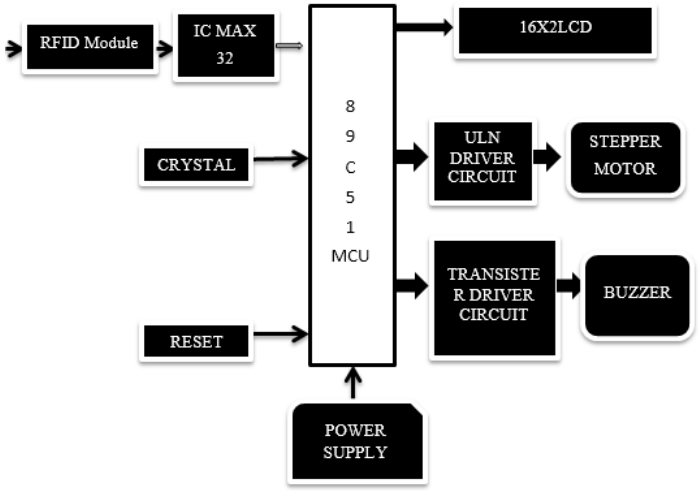

Figure. 5. Architecture of RFID Security System.

The output is taken from the additional port pins. The micro controller will analyze the input data of tag with stored data of the certified person and ports the output pin either to low or high. The data from the receiver module is sent to the relay which stands as the switch to the load. Relay is an electromechanical device. When the 5v signal is given to the circuit then magnetic energy will be produced and this magnetic energy will drive the switch from the NC point to the NO and a current passes through the motor and letting it to work to open a door.

3.9 RFID advantages

RFID advantages are given below:

- Reader can read and write data to RFID tags without any direct communication and no line of complication problem.
- Data from the different RFID tags are accessed by the reader by radio waves.
- No maintenance costs; RFID can work under different atmospheres and can be utilized efficiently for over 10 years.
- Fast read and write with the duration taken for read/write being a few milliseconds.
- Future generation RFID tags are made with excellent memory capabilities ranging from 16 - 64 Kbytes which is highly efficient than a typical barcode.
- RFID tags can work with GPRS and has been used for tracking.
- RFID tags can also integrate with other technologies. For example, it is used with wireless sensor net-works for better connectivity.

3.10 RFID Security

The principal and ultimate security issue of RFID technology is that anyone can access the RFID data because there is no line of sight complication that will be capable to gather data. Apart from that, people are copying RFID tags and using them just as the way it was done for credit cards before. Protecting effective copying of RFID tags are still an open and challenging issue for the next generation network infrastructures. Criminals with RFID readers could scan clusters for efficient value of bank notes. Also terrorists could scan digital passports to target particular nationalities.

Currently the research is on-going on RFID malware. RFID technology malware can be categorized into three different categories:

- Exploits,
- Worms, and
- Viruses.

RFID exploits are conventional hacking attacks that are identical to those found on the Internet like buffer overflows, code insertion, and SQL injection attacks. RFID worms and viruses are generally RFID exploits that copy the original exploit code to newly appearing RFID tags. The main difference between these two is that RFID worms trust on network connections whereas RFID viruses do not.

4 Near Field Communication vs. Far Field Communication for the Future Generation Network Infrastructures

Near Field Communication and Far field Communication both fall in the category of Radio Frequency Identification. In this part of study we are trying to differentiate the implementation issues of NFC and FFC on this basis of Radio Frequency Identification.

Near-field communication: The antennas of RFID reader transmit electromagnetic radiation or what we can say radio waves. So, if the RFID tag is in the range of the space complete wavelength of the reader, then under some conditions it is spoken to be in the "near field" (as with various RFID terms, illustrations are not properly identified). If in case, RFID tag is more than the distance of one complete wavelength across, then it is said to be in the "far field." The signal of the near field wireless communication technology blights as the cube of distance from the antenna, while as, signal of the far field wireless communication technology blights as the square of the distance from the antenna. Accordingly, passive RFID systems that commit on near-field communication (Normally L and HF

systems) have a lesser read range in comparison to those that utilize far field communication (UHF and microwave systems).

Far Field Communication -- In Far Field Communication an interrogator antenna the tag are connected under one full wavelength of the carrier wave. The far field signal blights as the square of distance from the antenna, and is generally utilized in Ultra High Frequency and Microwave systems. Far Field Communication manipulates a backscatter radio link [http://rfidsoup.pbwiki.com/Far+Field+Communication]. RFID reader antennas transmit electromagnetic radiation (radio waves). Accordingly, when the RFID tag is outside of one full wavelength of the reader, it is called to be in the "far field." If it is within one full wavelength away, it is called to be in the "near field." The far field blights as the square of the distance from the antenna, when the near field signal blights as the cube of distance from the antenna. Thus, passive RFID systems that commit on far field communications (particularly UHF and microwave systems) have a greater read range than those that utilize near field communications (normally low- and high-frequency systems).

Finally, we will provide the comparison survey of both these applications for the next generation network infrastructures to fulfill the aim of the methodology and implement the socio- technical undercurrent's for the future generation network standards.

Table 7. Comparison of NFC vs. FFC on the basis of Technology.

S. NO.	Attributes	NFC (HF)	FFC (UHF)	Remarks
1	Collision	Rare	Rare, Avoided by	No collision of reading tags and readers in NFC. In FFC, It is avoided through standardized algorithms approved by GS1 and GS2
2	Form factors of Design	Standardized	Customizable	UHF can be tamper proof windshield tags to avoid theft or misuse
3	Communication Protocols	Standardized	Proprietary and open	Development effort is more in UHF
4	Data Transfer Speed	Low	Fast	Faster speed gives faster processing in UHF
6	Environmental Factors	Resistant to water/metal	Read range affected by water/metal	UHF has effects on read range due to interference by metallic or liquid platform unlike HF due to working principle difference
7	Working Principle	EM Field interaction	Backscattering of EM waves	Field interaction can happen in closure distances only (NFC) no EM emission in HF unlike UHF
8	Security/Authentication	Data stored in tag itself	Information stored and server authentication required	NFC is more Vulnerable for data theft
9	Range Control	Up to 1 Meter	Up to 12 meters	Better Range, Better Visibility, Better Operations
10	Ambient Factors (Temperature, Humidity, Ruggedness)	Taken care by manufacturer following CE and GS standards	Taken Care by manufacturer following CE and GS standards	Similar in both HF and UHF. IP 42 AND IP 65 protection

Table above showing comparison on the basis of Technology, further more now we are showing the comparison on the basis of Operations and Management of NFC and FFC for the Next Generation Network Infrastructures.

Table 8. Showing Comparison on the basis of Operations and Management

S. NO.	Attributes	NFC (HF)	FFC (UHF)	Remarks
1	Waiting Time	More	Less	Due to read range and faster data transfer, UHF has its advantages over HF based systems
2	Design	Standardized	Tamper Proof	UHF tags cannot be removed, misused or stolen
3	Security	All information stored in card only	Only unique ID and basic data Stored in tags, server verification also required	2 levels of verification process makes UHF more safer
4	Boom Barrier Operation	Complete cycle for each pass	No need to complete a full cycle for each pass. Auto response through loop detectors or anti-crash sensors	Life of boom barrier and energy saving is more in FFC in comparison to NFC
5	Ease-of-use for users	Stop, roll down window, go near the reader	Automatic Reading from distance	A user needs to stop at closure distance to reach the reader or step down from the car to authenticate in NFC, No such hassles in FFC
6	Queue management	One by one reading form close proximity, no multiple reading capabilities	Automated reading from controlled distance and Multiple reading capabilities	Queue Management becomes faster in FFC due to automated reading and multiple reading capabilities
7	Future Prospects	1) Cannot be integrated and used in large and high transition parking guidance or Asset mgt (No RTLS) or Guard patrolling systems 2) Not suited for locating parked cars in busy and large parking	1) Can be integrating and used in large and high transition parking guidance system or Asset Tracking systems or Guard Patrolling systems (on demand –Auto RTLS) 2) Can be utilized for locating your parked car	1) Auto parking guidance system during peak hours requires a high speed and long range technology to avoid conjunction i.e., FFC based systems 2) Future Integration for other desired solution can be possible with Long Range Technologies only i.e. on demand-Automated Real Time Asset Tracking or guard patrolling systems 3) Location search for parked car for future

Comparison between two wireless technologies (NFC vs. FFC) with respect to Economics and Management.

Table 9. Comparison of NFC VS. FFC on basis of Economics and Environment.

S. NO.	Attributes	NFC (HF)	FFC(UHF)	Remarks
1	Cost Of Technology	Readers are of same price, cards are costlier	Cheaper tags/cards	1) Readers of both HF and UHF come at almost same price but UHF tags are cheaper than HF cards 2) Price factor is necessary to consider for consumables as it is needed continuously
2	Green Concept	More Co2 and Co emission during entry-exit and parking slot search, leading to more cost to control and maintain air ambience	Lesser waiting time leads to lessor CO2 and CO emissions	FFC based solution should be preferred for Advent's "Green Technology Philosophy"
3	Service and Support	Readily Available	Readily Available	Hardware components, spare parts, servicing options etc. are readily available for both the technologies
4	Cost of Operation	Slightly Cheaper	Slightly Cheaper	UHF is slightly higher due to slightly higher energy consumption as it works on backscatter principle unlike HF
5	Fuel Consumption	More fuel consumption due more waiting time	Better fuel management benefits during entry-exit of cars and automatic parking guidance in parking lots	FFC certainly has advantages over NFC in Fuel ROI
6	Cost of maintenance	Cheaper	Moderate	Maintenance of UHF based systems are relatively higher than HF

5 CHALLENGES AND DISCUSSION

RFID technology faces numerous implementation challenges. The major challenges include technological capability, Universal regularity, government rule and regulations, and cost as summarized in Table 10 and described below:

Table 10. RFID implementation Challenges

Levels	Challenges
Fundamental	• High Capital costs • Challenges in finding the ROI • Challenges in finding the "drivers" for adoption.
Technical	• Imperfect read-rates • Unproven systems • Difficulties with capturing low-cost tags • Uncertainty about the role of the middleware • Lack of in-house experts to implement RFID
Security	• Issues regarding the compromise of data during wireless transmission • Uncertainty around security of data storage and physical security of storage site
Privacy Issues/ Govt. Regulations	• Privacy issues and the potential for legislation • Uncertainty around Standards

At present, the NFC technology has reached a level where commercial launch preparation can begin and should be established. However, to some extent definite standards for NFC services are still missing:

- The scarcity of an ultimate conclusive approach for the development of NFC services originates in a vital conflict between several involved key actors including mobile phone manufactures, network operators, banks and other service providers: every party indeed tries to enforce its interests and wants to play a major role in the flow of the application scenario and the associating acquisition of big money.
- Third-party income producers, cognate banks and different financial associations, need to anchor NFC applications in unbiased space on the mobile phones, while network operators of course want to charge clients for presenting services hosted in protected atmosphere on the UICC. Due to different workloads in NFC applications, they are also busy in custody of the highlighted wireless network infrastructures and can thus control any SMS-based remote over-the-air authority potentials that might be utilized to efficiently design or modernize NFC services on the handset.
- The mobile phone manufacturers on the other hand decide which sort of NFC hardware and which alternative forms of dedicated Secure Element chips are actually implemented in the handset. And on higher layers, of course also the phone's operating system needs to provide appropriate NFC support.
- Google already offers mature NFC interfaces for developers within their own Android operating system and - in partnership with several banks and the assistance of a handset manufacturer – managed to publish a fist qualified application for mobile NFC payment. Competitors from Apple and Microsoft indeed also announced plans to develop smartphones with NFC backing in the next generation, but the
- Thing is that, it is still uncertain how exactly their concept will look like. Nevertheless, this means that NFC applications are still handset specific.
- A simple, dynamic and platform-independent framework is missing and difficult to realize. In a certain way though, a collaboration of stakeholder, in particular phone manufacturers and network operators, is definitely needed for developing sophisticated and usable NFC services for the mass market.
- Mobilization and authenticity of NFC applications are perhaps the ultimate determinants of the user understanding in day to day use of the NFC technology and accordingly crucial keys to its prosperity.

6 Conclusion

RFID is still in an emerging stage and furthermore is in the pipeline in terms of up to date applications, Various Researches can be done through this technology. Between applications which have been developed earlier, RFID tags are being utilized in dressing for invoice and security issues. RFID tags are embedded inside animals for tracking concerns. RFID tags placed in dresses can be used to be aware about the number of hours an employee spends to complete a particular its work. There are numerous organizations that are pro-testing against the use of RFID to track people fearing the impact on people's social life and privacy. Clearly the extent to which use RFID is to be used is still an open debate. A large type of articles on RFID tags are ongoing including on embedding these with different devices, particularly on mobile devices. RFID users and makers are looking for complete standardization and requirement of RFID. As the cost of applications sink too and technological enhancements continue to exist, RFID technology is supposed to grow economically and technically more feasible and influence our daily lives when more applications are being developed. RFID technology authorize users to enhance perfection, presents superior data flow management, higher data processing speeds, amplified security and minimization of bugs through authentication and automation. It further helps concluding cost savings and ROI from both implementer and user standpoint. In order to conclude these enhancements, it is important that an RFID Professional knows and understand the distinct differences between HF and UHF RFID to execute the accurate abilities and fluctuations to assemble the particular application requirements.

Near Field communication technology allows its users to conceptualize and undergo a brand new and inspiring universe. It has facilitated its users with a variety of applications. However, there outlets two faces of coin, NFC technology also got affected from one such coin as well. It follows various particular threats that don't allow users to take a good use of it. This study describes different applications scenarios of RFID, NFC and FFC, and outlines series of threats and its respective counter measures to protect these short-range wireless technologies. These deportments can be used to provide security to applications using NFC technology and also attract more users to use it without any problem statement. Further, the paper would be very helpful for new learners to understand RFID, NFC, FFC Next Generation wireless technologies, its applications, threats and security constructs used for protecting it. It also animates researchers to launch some global assistance for securing these wireless technologies from threats to build user's confidence in technology to use it further for the Future Generation Wireless Network Infrastructures.

ACKNOWLEDGEMENT

We are thankful to all the Faculty members of Computer Science and Engineering Department, Shri Ramswaroop Memorial University Lucknow Uttar Pradesh for their motivation and continuous support. Our special vote of thanks to Dr. Bineet Gupta for their valuable suggestions and contributions.

REFERENCES

[1] Sanjay Ahuja, Pavan Potti "An Introduction to RFID Technology", School of Computing, University of North Florida, Jacksonville, Florida Communications and Network, 2010.

[2] Simon Burkard "Near Field Communication in Smartphones", Master Student, Computer Engineering Dep. of Telecommunication Systems, Service-centric Networking, Berlin Institute of Technology, Germany.

[3] Chetna Bajaj, "Near Field Communication", International Journal of Advanced Research in Computer Science and Software Engineering, Department of Computer Science & Engineering, Ambedkar Institute of Advanced Communication Technologies and Research, Delhi, India, Volume 4, Issue 8, August 2014.

[4] IEEE USA "The State of RFID Implementation and Its Policy Implications: An IEEE-USA White Paper", 15 April 2009.

[5] Vipul Chawla and Dong Sam Ha, "An Overview of Passive RFID", Virginia Polytechnic Institute and State University, IEEE Applications & Practice, September 2007.

[6] Vibhor Sharma, Preeti Gussian, Prashant Kumar "Near Field Communication", Department of Computer Science & Engineering Tula's Institute, The Engineering and Management College, Dehradun, Uttarakhand 248001, India, Conference on Advances in Communication and Control Systems 2013 (CAC2S 2013).

[7] Arun N. Nambiar "RFID Technology: A Review of its Applications", Proceedings of the World Congress on Engineering and Computer Science, San Francisco, USA. 2009 Vol II WCECS 2009, October 20-22, 2009,

[8] K.Srinivasa Ravi, G.H.Varun, T.Vamsi, P.Pratyusha "RFID Based Security System", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-5, April 2013.

[9] Mohsen Attaran, "Critical Success Factors and Challenges of Implementing RFID in Supply Chain Management", California State University, Bakersfield, CA, USA. Journal of Supply Chain and Operations Management, Volume 10, Number 1, February 2012.

[10] Xiaozheng Lai, Zeming Xie, and Xuanliang Cen, "Compact Loop Antenna for Near-Field and Far-Field UHF RFID Applications", School of Computer Science & Engineering, South China University of Technology, Guangzhou 510006, China, Progress In Electromagnetics Research C,Vol-37, 171-182, 2013.

[11] Yuan Yao, Junsheng Yu, and Xiaodong Chen, "Study on the Optically Transparent Near-Field and Far-Field RFID Reader Antenna", Beijing Key Laboratory of Work Safety Intelligent Monitoring, School of Electronic Engineering, Beijing University of Posts and Telecommunications, No. 10 Xitucheng Road, Beijing, China, Hindawi Publishing Corporation International Journal of Antennas and Propagation, Article ID 149051, Volume 2014.

[12] M. MABROUK , M. DHAOUADI, T.P. VUONG , A.C DE SOUZA, A. GHAZEL, "A Broadband UHF TAG Antenna For Near-Field and Far-Field RFID Communications", Laboratoire GRESCOM, SUPCOM de Tunis, University de Carthage, RADIOENGINEERING, VOL. 23, NO.4, DECEMBER 2014 – ERRATA.

[13] Jignesh Patel, Badal Kothari, "Near Field Communication - The Future Technology For An Interactive World", Int. J. Engg. Res. & Sci. & Tech. 2013 ISSN 2319-5991 Vol. 2, No. 2, May 2013.

[14] Gowher Mushtaq, Shashank Singh, Neeraj Kumar Tiwari, "To Study the Energy Efficient Deportments of Existing Attributes for Next Generation Network Infrastructures", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-4 Issue-4, April 2015.

[15] Mohammad Umair Yaqub, Umair Ahmad Shaikh, "Near Field Communication -Its Applications and Implementation in K.S.A.", King Fahd University of Petroleum & Minerals, 13th of February 2013.

[16] Asawari Dudwadkar, Akhil Gore, Tushar Nachnani, Harshil Sabhnani, "Near Field Communication in Mobile Phones", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-3, Issue-1, October 2013.

[17] Tomasz Dlugosz, Hubert Trzaska, "How to Measure in the Near Field and in the Far Field", Wroclaw University of Technology Institute of Telecommunications, Teleinformatics and Acoustics, Wyspianskiego, Wroclaw, Poland, Communication and Network, 2, 65-68, 2010.

[18] Coskun, V., Ozdenizci, B., & Ok, K, "A Survey on Near Field Communication (NFC) Technology". Wireless personal communications, 71(3), 2259-2294, 2013.

[19] Ari Juels, "RFID Security and Privacy: A Research Survey", IEEE Journal on Selected Areas in Communications, VOL. 24, NO. 2, February 2006.