*IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)*
*e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 9, Issue 1, Ver. I (Jan. 2014), PP 06-10*
*www.iosrjournals.org*

# A Novel Security System using near Field Identification (NFID)

Shivaraman Ilango
*Health Care Technology and Innovation Centre IIT Madras Research Park*

***Abstract:*** *Near Field Communication (NFC) is one of the latest wireless communication technologies, making possible variety of novel services particular in the security aspect. This paper presents an idea to implement a security system using a new technology called the Near Field Identification (NFID) which uses the combined principle of NFC and RFID (Radio frequency Identification). The security system thus developed will have a wide advantage over the existing biometric systems that are in practice and will provide a highly secure environment in the near future.*
***Keywords****: Amplifier, LED, NFID, NFC, RFID, Security*

## I. Introduction

NFC is a short-range high frequency wireless communication technology that enables the exchange of data between devices over about a 10 cm distance. NFC is an upgrade of the existing proximity card standard (RFID) that combines the interface of a smartcard and a reader into a single device. It allows users to seamlessly share content between digital devices, pay bills wirelessly or even use their cellphone as an electronic traveling ticket on existing contactless infrastructure already in use for public transportation. The significant advantage of NFC over Bluetooth is the shorter set-up time. Instead of performing manual configurations to identify Bluetooth devices, the connection between two NFC devices is established at once (under a 1/10 second).Due to its shorter range, NFC provides a higher degree of security than Bluetooth and makes NFC suitable for crowded areas where correlating a signal with its transmitting physical device (and by extension, its user) might otherwise prove impossible .NFC can also work when one of the devices is not powered by a battery (e.g. on a phone that may be turned off, a contactless smart credit card, etc.).

Radio-frequency identification (RFID) is the use of a wireless non-contact system that uses radio-frequency electromagnetic fields to transfer data from a tag attached to an object, for the purpose of automatic identification and tracking. Some tags require no battery and are powered and read at short ranges via magnetic fields (electromagnetic induction). Others use a local power source and emit radio waves (electromagnetic radiation at radio frequencies). The tag contains electronically stored information which may be read from up to several meters away. Unlike a bar code, the tag does not need to be within line of sight of the reader and may be embedded in the tracked object. RFID tags are used in many industries. An RFID tag attached to an automobile during production can be used to track its progress through the assembly line RFID systems typically come in three configurations. One is a Passive Reader Active Tag (PRAT) system that has a passive reader which only receives radio signals from active tags (battery operated, transmit only). The reception range of a PRAT system reader can be adjusted from 1- 2,000 feet, Thereby allowing for great flexibility in applications such as asset protection and supervision. Another configuration is an Active Reader Passive Tag (ARPT) system that has an active reader, which transmits interrogator signals and also receives authentication replies from passive tags. Finally, there is the Active Reader Active Tag (ARAT) system in which active tags are awoken with an interrogator signal from the active reader. A variation of this system could also use a Battery Assisted Passive (BAP) tag which acts like a passive tag but has a small battery to power the tag's return reporting signal. RFID tags can be either passive, active or battery assisted passive. An active tag has an on-board battery and periodically transmits its ID signal. A battery assisted passive (BAP) has a small battery on board and is activated when in the presence of a RFID reader. A passive tag is cheaper and smaller because it has no battery. Instead, the tag uses the radio energy transmitted by the reader as its energy source. The interrogator must be close for RF field to be strong enough to transfer sufficient power to the tag. Since tags have individual serial numbers, the RFID system design can discriminate several tags that might be within the range of the RFID reader and read them simultaneously. Tags may either be read-only, having a factory-assigned serial number that is used as a key into a database, or may be read/write, where object-specific data can be written into the tag by the system user.. The tag's information is stored electronically in a non-volatile memory. The RFID tag includes a small RF transmitter and receiver. An RFID reader transmits an encoded radio signal to interrogate the tag. The tag receives the message and responds with its identification information. This may be only a unique tag serial number, or may be product-related information such as a stock number, lot or batch number, production date, or other specific information. 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.

In the NFID Scenario we have an active card with Encoders that acts like a transmitter and the receiving unit with a decoder. The active card that is with the person who is seeking an entry into a highly confidential area is preprogrammed with the personal details of the person. As the person seeks entry, the receiving unit with the decoder starts to decode the details by reading the active card from a particular distance and only when the data matches the details of the person is the door opened automatically for a period of 5 seconds. The way this technology works will be explained in detail in the following paper.

## II. Existing System

A bit is the smallest unit of information that can be represented and has only two states:1 and 0. This means that only two states can be represented by systems based upon a1-bit transponder: 'transponder in interrogation zone' and 'no transponder in interrogation zone'. Despite this limitation, 1-bit transponders are very widespread — their main field of application is in electronic anti-theft devices in shops (EAS, electronic article surveillance).An EAS system is made up of the following components: the antenna of a 'reader or interrogator, the security element or tag, and an optional deactivation device for activating the tag after payment. In modern systems deactivation takes place when the price code is registered at the till. Some systems also incorporate an activator, which is used to reactivate the security element after deactivation. The main performance characteristic for all systems is the recognition or detection rate in relation to the gate width (maximum distance between transponder and interrogator antenna).The procedure for the inspection and testing of installed article surveillance systems is specified in the guideline VDI 4470 entitled 'Anti-theft systems for goods — detection gates. Inspection guidelines for customers'. This guideline contains definitions and testing procedures for the calculation of the detection rate and false alarm ratio. It can be used by the retail trade as the basis for sales contracts or for monitoring the performance of installed systems on an ongoing basis. For the product manufacturer, the Inspection Guidelines for Customers represents an effective benchmark in the development and optimization of integrated solutions for security projects.

### Radio frequency:

The radio frequency (RF) procedure is based upon LC resonant circuits adjusted to a defined resonant frequency fR. Early versions employed inductive resistors made of wound enameled copper wire with a soldered on capacitor in a plastic housing (hard tag). Modern systems employ coils etched between foils in the form of stick-on labels. To ensure that the damping resistance does not become too high and reduce the quality of the resonant circuit to an unacceptable level, the thickness of the aluminum conduction tracks on the 25 µm thick polyethylene foil must be at least 50µm. Intermediate foils of 10µm thickness are used to manufacture the capacitor plates. The reader (detector) generates a magnetic alternating field in the radio frequency Range. If the LC resonant circuit is moved into the vicinity of the magnetic Alternating field, energy from the alternating field can be induced in the resonant circuit via its coils (Faraday's law). If the frequency fG of the alternating field corresponds with the resonant frequency fR of the LC resonant circuit the resonant circuit produces a sympathetic oscillation. The current that flows in the resonant circuit as a result of this acts against its cause, i.e. it acts against the external magnetic alternating field. This effect is noticeable as a result of a small change in the voltage drop across the transmitter's generator coil and ultimately leads to a weakening of the measurable magnetic field strength. A change to the induced voltage can also be detected in an optional sensor coil as soon as a resonant oscillating circuit is brought into the magnetic field of the generator coil. The relative magnitude of this dip is dependent upon the gap between the two coils (generator coil — security element, security element — sensor coil) and the quality Q of the induced resonant circuit (in the security element).The relative magnitude of the changes in voltage at the generator and sensor coils is generally very low and thus difficult to detect. However, the signal should be as clear as possible so that the security element can be reliably detected. This is achieved using a bit of a trick: the frequency of the magnetic field generated is not constant, it is 'swept'. This means that the generator frequency continuously crosses the range between minimum and maximum. The frequency range available to the swept systems is 8.2MHz ±10% .Whenever the swept generator frequency exactly corresponds with the resonant frequency of the resonant circuit (in the transponder), the transponder begins to oscillate, producing a clear dip in the voltages at the generator and sensor coils. Frequency tolerances of the security element, which depend upon manufacturing tolerances and vary in the presence of a metallic environment, no longer play a role as a result of the 'scanning' of the entire frequency range. Because the tags are not removed at the till, they must be altered so that they do not activate the anti-theft system. To achieve this, the cashier places the protected product into a device — the deactivator — that generates a sufficiently high magnetic field that the induced voltage destroys the foil capacitor of the transponder. The capacitors are designed with intentional short- circuit points. The breakdown of the capacitors is irreversible and detunes the resonant circuit to such a degree that this can no longer be excited by the sweep signal.

## III. Implementation

The Near field identification technique combines the principle of both RFID (Radio Frequency Identification) and NFC (Near Field Communication) for authorized entry in to a sophisticated environment with various levels of authentication This near field identification is implemented by using an encoder (HT12E) Decoder (HT12D),RF transmitter which transmits signals of 315Mhz frequency and RF receiver receives signals of 315Mhz,434Mhz and 402.52Mhz frequency,9v(volt)DC power supply, alarm. The range of transmission and receiving of signals can be varied by changing the frequency of the transmitter and receiving unit.

### 3.1 NFID TRANSMITTER (CARD)

The NFID Card has an Encoder (HT12E) in which the personal identification of the employee has been programmed using keil c. the encoder is connected to the RF transmitter. A 9v dc supply acts a source of power for the NFID card.The NFID Card is different for different employees based on the programming done on the encoder.

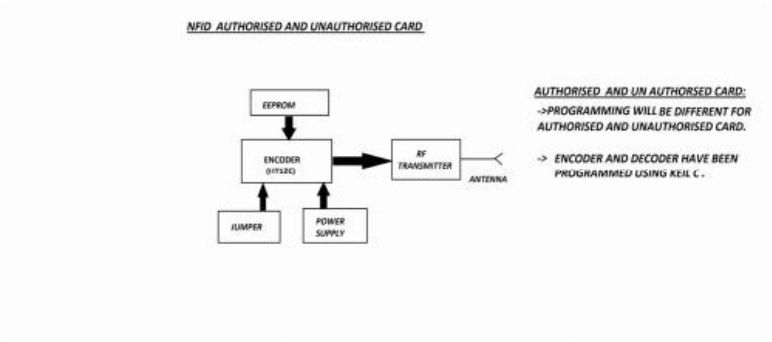


Fig 1

**3.2 NFID DETECTOR:**

The NFID Receiver is fitted to the fixed on the door or valve adjacent to the door to which the employee wearing the transmitter unit is seeking entry. It has an Decoder (HT12D).The Decoder decodes the program from the NFID Card and if the program matches the value will be actuated and the door will be open and if the program is unmatched the alarm will be blown.

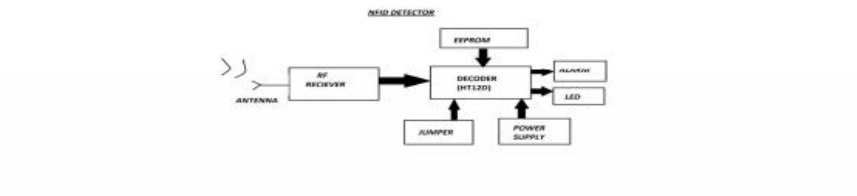


Fig. 2

Fig 1

### 3.2 NFID DETECTOR:

The NFID Receiver is fitted to the fixed on the door or valve adjacent to the door to which the employee wearing the transmitter unit is seeking entry. It has an Decoder (HT12D).The Decoder decodes the program from the NFID Card and if the program matches the value will be actuated and the door will be open and if the program is unmatched the alarm will be blown

Fig. 2

**3.3 OVERALL SECURITY SYSTEM**

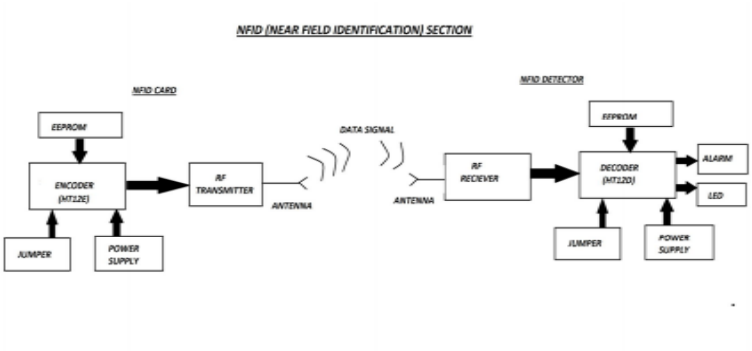


Fig.3

The working of this entire unit is quite interesting. The NFID card is programmed with the personal details of the person in the encoder. This card also consisting of a RF Transmitter antenna transmits data to the detector unit when powered on. The detector Unit consist of a decoder which decodes the data send by the transmitter and only when the data matches the data present in the detector unit , the person who is seeking entry is allowed to enter by the automatic opening of the doors on which the detector unit is fixed. There are two LED units in the detector section, a red LED and a GREEN led. Either of the LED's blinks rapidly depending upon the data matching. If an authorized person is seeking entry then the Green Led starts blinking rapidly. At a point where the intensity is maximum, the output of the LED is amplified and programmed to close a solenoid valve that runs a motor which operates the automatic opening and closing of the doors. When an unauthorized person seeks entry it turns on the Red LED and the alarm that is connected is triggered which alerts the people in the control room. Thus this security system has an edge over the existing biometric systems and does not need a security monitoring continuously.

### 3.3 OVERALL SECURITY SYSTEM

Fig.3

The working of this entire unit is quite interesting. The NFID card is programmed with the personal details of the person in the encoder. This card also consisting of a RF Transmitter antenna transmits data to the detector unit when powered on. The detector Unit consist of a decoder which decodes the data send by the transmitter and only when the data matches the data present in the detector unit , the person who is seeking entry is allowed to enter by the automatic opening of the doors on which the detector unit is fixed. There are two LED units in the detector section, a red LED and a GREEN led. Either of the LED's blinks rapidly depending upon the data matching. If an authorized person is seeking entry then the Green Led starts blinking rapidly. At a point where the intensity is maximum, the output of the LED is amplified and programmed to close a solenoid valve that runs a motor which operates the automatic opening and closing of the doors. When an unauthorized person seeks entry it turns on the Red LED and the alarm that is connected is triggered which alerts the people in the control room. Thus this security system has an edge over the existing biometric systems and does not need a security monitoring continuously.

## IV. Conclusion

This paper presents a non-contactless, highly profound security system that does not require the continuous monitoring by the security personnel's which will provide an added advantage when compared to the already existing biometric security systems. This healthy invention when developed further with the advancement in Science and Technology will raise the standards of security systems at present thus giving a new dimension to the field of wireless security systems.

## References

[1] W. Webb, Wireless Communications: The Future John Wiley & Sons, 2007. Gelenbe, E. (2006)
[2] Near Field Communication and the NFC Forum: The Keys to Truly Interoperable Communications White Paper, NFC Forum, 2007
[3] B. Benyó, B. Sódor, A. Vilmos, G. FördĘs,"A novel virtual machine based approach for hosting NFC services on mobile devices" WMNC 2010.
[4] Benyó B, Sódor B, Kovács L, Homlok J, FördĘs G: Security issues of service installation on a multi-application NFC environment. 14th IEEE Int. Conference on Intelligent Engineering Systems (INES 2010).
[5] K. Finkenzeller, RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and IdentificationJ. Wiley & S., 2003
[6] Short Form Specification, "Near Field Communication PN531- C based Transmission module", Philips Semiconductors, February 2004.