Conditional Privacy Preserving Security Protocol for NFC Applications

Nithyanand Singh
Dept. of ECE, RRIT, Bangalore, Karnataka, India

Avijit Maity
Dept. of ECE, RRIT, Bangalore, Karnataka, India

Rajesha N
Dept. of ECE, RRIT, Bangalore, Karnataka, India

Abstract - NFC (Near field Communication) is a short-range wireless communication technology whose VGF technology distance is around 4 inches, and it operates in the 13.56MHz frequency band at a speed of 106Kbps to 424Kbps. The combination of NFC with smart devices resulted in widening the range of NFC, which includes data exchange, service discovery, connection, e-payment, and ticketing. It is expected to replace credit cards in electronic payment, especially. According to based payment services is expected to increase by 11.3 times from $316 million in 2010 to $3.572 billion in 2015, and Juniper research predicted that the global NFC payment market size would be increased to $180 billion in 2017. To use NFC in electronic payment, security is a prerequisite to be addressed. Presently, NFC security standards define data exchange format, tag types, and security protocols, centering on NFC forum. It is expressly stipulated in the NFC security standards that key agreement is required for secret communications between users. In the process of key agreement, both users should exchange their public keys. The public key is received from CA (Certificate Authority), and it uses a fixed value until reissued. Malicious internal attackers can create profiles of users through the acquisition of public keys of other users in the process of key agreement. If NFC is used in e-payment in this way, the privacy of users can be infringed through profiles created by attackers. Suppose Alice purchases items such as cloths, food, and medicine several times at a supermarket, the supermarket can get information about her tastes, preferences, and health conditions. The collected information can help her to purchase products more efficiently, but it may contain information that nobody wants to announce to others such as his or her health conditions.

Keywords: NFC, GSM, RFID

I. INTRODUCTION

The idea of this project is to develop the prevention of theft of the ATM card and to control the usage of the ATM card by unauthorized person. The additional feature of this project is that no transaction can be done without the knowledge of the respective card holder for the cause that NFC transactions are being implemented. The description of the project is as follows; whenever the transaction has to be done, the RFID card is inserted inside the ATM machine and NFC devices are made to interact with some of the legacy systems. Granting that both RFID and NFC device is found to be accurate, a message is received to the mobile phone of the rightful proprietor with a pin number of four digits. This number is entered in the ATM machine. In case of password being correct it moves on to the next level of money transaction, asking for the money withdrawal. Scenario like, the password is found to be defective, next in order of time image of highwayman is captured and passage out will be locked.

The main objective of this project is to develop an embedded system, which is used for security applications. In this security system the specific persons can only enter; by using this embedded system we can give access to the authorized people through the finger print modules and keypads. The system is programmable we can change the data of the authorized people in the data base of the embedded system; we can access the data on the embedded system on to computer. The complete code for the embedded system is going to be developed using C-Language. The embedded system is going to be developed based on microcontroller; whenever the person puts his finger on the reader the system will detect the authorized persons then it asks for pin and gets the message to authorized persons mobile through the GSM technology. Fingerprint reader module will be interfaced to the microcontroller and the pin is entered through the either mobile or keypad.

The Rest of the paper is as follows. Section 1 describes the Introduction. Section 2 defines the Glide path. Section 3 defines the NFC protocol operation, Section 4 defines the security principle, Section 4 provides experimental setup and Section 6 conclude the topic.

II. GLIDE PATH

Our Secure Mobile Wallet is the product belonging to the latest technology trends in mobile communications and IT security. As the client application of the larger system, SAFETM, Secure Mobile Wallet will introduce convenience, functionality and security in financial mobile transaction. The aim of the design is to provide people a more flexible way to use cash and credit cards securely. The advantage of this approach is that user interfaces are very nice and data are strongly protected in the applets. This approach is very convenient and application level end-to-end security. Improve the consumer's shopping experience.

Receiver

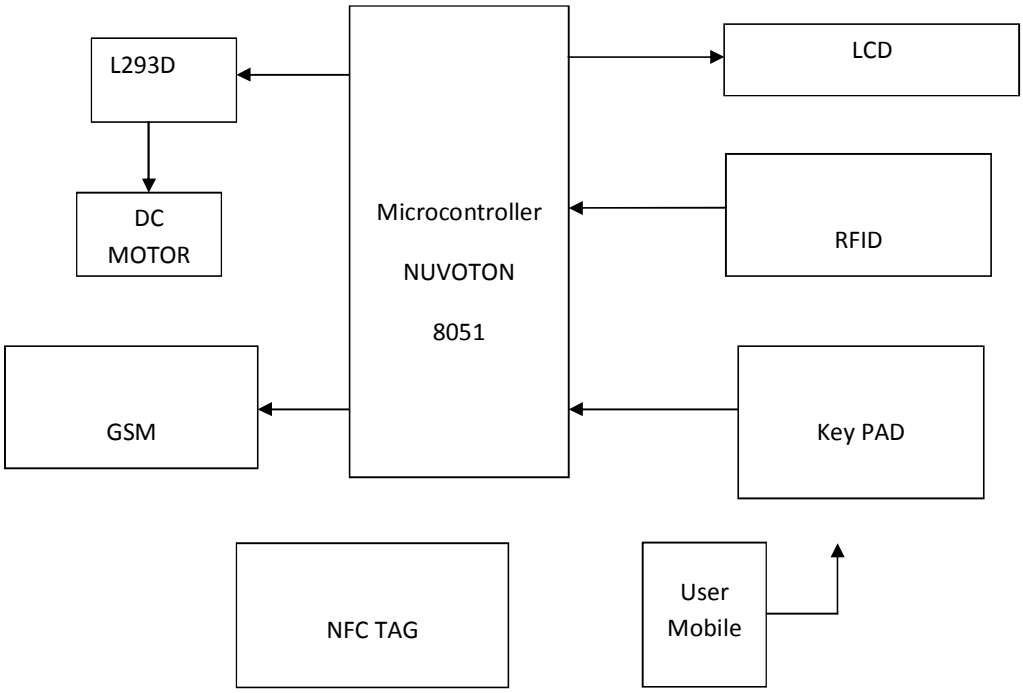

Figure 1: Block diagram representation of proposed module

2.1 Interfacing the GSM Module with Microcontroller

The Global System for Mobile communications (GSM: originally from Groupe Special Mobile) is the most popular standard for mobile phones in the world. GSM service is used by over 2 billion people across more than 212 countries and territories. Its ubiquity makes international roaming very common between mobile phone operators, enabling subscribers to use their phones in many parts of the world. GSM differs significantly from its predecessors in that both signaling and speech channels are digital call quality, and so is considered a second generation (2G) mobile phone system. This has also meant that data communication was built into the system from the 3rd Generation Partnership Project (3GPP).

A SIM card is inserted to the GSM module. After checking as shown in the steps above, RS232 cable is directly connected between DB9 of the module and the DB9 on the controller port. This establishes the serial communication between them. The GSM commands embedded in the controller takes care to communicate with the GSM Module via RS232 cable-MAX232-Serial I/O pins of the MAX232.

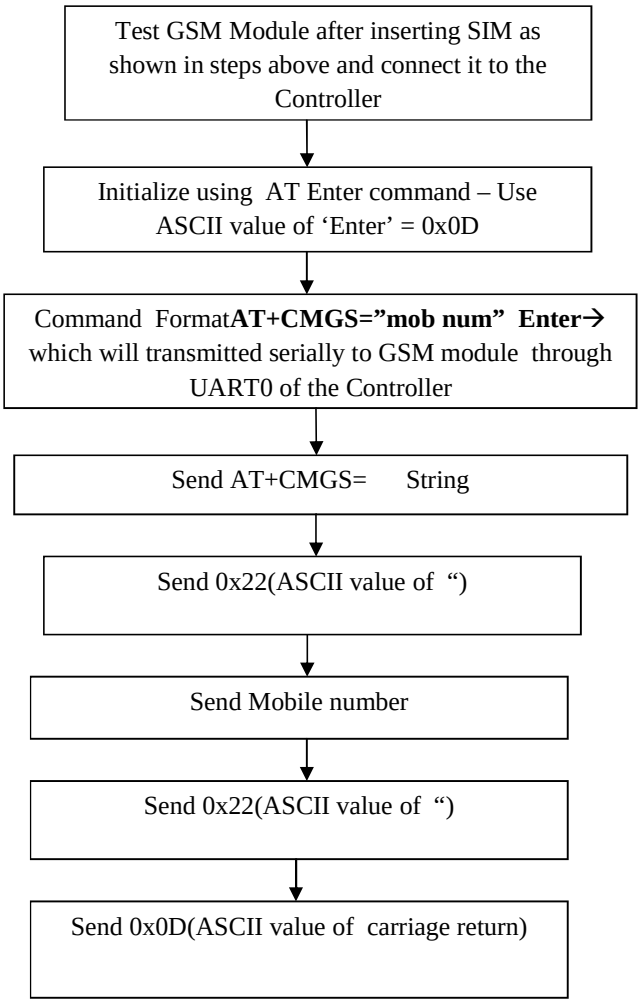

Figure 2: GSM Send SMS Flow Chart

2.1.1 Steps to test the GSM Module

We can use the PC Hyper Terminal to interact with the GSM Module.

1. First insert the SIM card to the GSM Module,
2. Connect the Serial cable –RS232 to the PC via DB9 pin connector on the GSM Module.
3. Give the power supply. The power supply indicating LED will be ON continuously.
4. Another LED on the Module starts blinking to indicate the availability of network.
   If the network is available then the delay between the blinking is less.
   If the network is not available then the delay between the blinking is more.
5. Each GSM modem will have a unique id called IMEI.
6. Open Hyper Terminal in the PC , apply the below settings

Connect using	→	COM1
Bits per second	→	9600
Data bits	→	8
Parity	→	None
Stop bits	→	1
Flow control	→	None

7. Type AT on HyperTerminal and press ENTER → OK will be display as a response from the GSM Module.
   AT
   OK

III. NFC PROTOCOL

This paper gives a general overview of Near Field Communication (NFC) technology with a special focus on safety and security. First, an introduction is provided on how NFC works. The associated hardware structure, standard communication methods, and the relevant international standards for NFC are discussed. In the main section, this work examines the security and safety risks of NFC, summarizes built-in measures regarding security and safety and also suggests a principal protocol for safety integrated communication with NFC.Finally, this work shows some applications, with focus given to aid organizations, which would benefit greatly from the use of NFC technology.

NFC is a Radio Frequency (RF) technology for communication over short distances up to about 10cm. It is mainly a logical advancement of Radio Frequency Identification (RFID). The history of RFID reaches back to the Second World War, where the British Air force tagged their planes with suitcase-sized devices to establish friend-enemy detection. The first commercial release came in the 1960's: 1 bit RFID for securing goods in shops, which is still widely used. In the 1990's RFID became more and more common e.g. for admission control systems or toll systems. In 2002, NFC was developed by NXP Semiconductors and Sony. In general, NFC is compatible with existing RFID systems, but its architecture is different in principle. While RFID has only a reader - tag structure, an NFC device can be both reader and transmitter. In 2004, for better standardization the NFC-Forum was founded by the two developing companies. The forum now has about 140 members [17]. After this, the most NFC relevant standards were released as European Computer Manufacturers Association (ECMA) standards before becoming an ISO/IEC standard, by a procedure called Fast-Track [12]. The first NFC-compatible mobile phones were distributed by Samsung and Nokia in 2005. In the same year the first field trials in payment with NFC started in France [12]. The world's first commercial rollout of NFC was in Austria. Mobilkom Austria, OEBB and Wiener Linien placed about 450 NFC tags at vending machines to support the customer, in buying tickets for the railway and underground via SMS. For the near future, commercial use of NFC technology is expected to increase.

This is due to the fact that three smart phone operating system / device manufacturers Apple (iPhone), Google (Android) and RIM (Blackberry) have announced plans to include NFC in their next products. Additionally, MasterCard, an international debit card company, is about to start its PayPass, an NFC based payment solution [15].

Operation Modes

The most important NFC standards, in relation to the operation modes, are ECMA-340: Near Field Communication Interface and Protocol (NFCIP-1) [16] and ECMA-352: Near Field Communication Interface and Protocol - 2 (NFCIP-2) [16]. NFCIP-1 combines the two RFID communication protocols: MIFARE (ISO/IEC 14443 Type A [15]) and FeliCa (JIS X 6319-4 [15]), and extends them with new communication possibilities and a new transport protocol. NFCIP-2 combines NFC with the functionality of RFID readers. This way NFC is compatible with most RFID devices [15].

Where RFID has strictly one or more passive components (tags) and one active component (reader), NFC breaks this up. For NFC devices it is possible to communicate with each other, acting as tag or as reader / writer. To ensure this, the NFC-Forum defines the following operation modes [16]: Peer to Peer Mode, Reader / Writer Mode and Card Emulation Mode. A systematic overview is given in Figure 3. Parts of the algorithms to determine which mode is used and to get knowledge of other NFC devices in range are defined in NFCIP-2.

Whereas most RFID readers are designed to be the only active devices in range, for NFC devices this assumption is not possible, therefore collision avoidance is used. Also the recognition speed of devices in range should stay beyond 200ms, for proper usability. Many NFC devices are mobile and therefore have a narrow power capacity, since higher recognition speed requires more energy. There will be always a compromise between the detection speed and the energy consumption

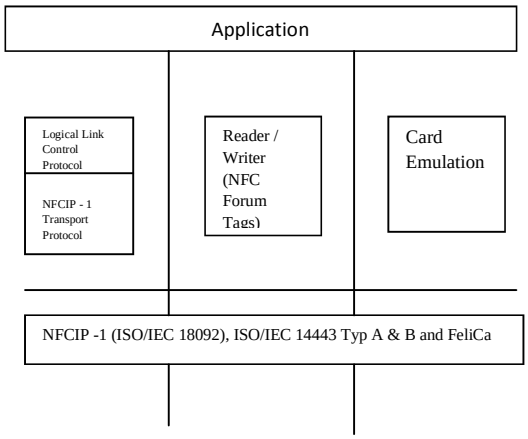

Figure 3: Systematic Overview of NFC

A. *Peer to Peer Mode:* Peer to Peer Mode enables communication between two NFC devices. The device which starts the communication is called Initiator, the other is called Target. The Peer to Peer Modes protocol stack is organized similar to the OSI Reference Model, but has only 4 Layers: Physical, Media Access Control (MAC), Logical Link Control (LLC) and Application. Physical and Application Layers are equal to the OSI Reference Model, MAC and LLC build the Data Link Layer of the OSI.

Table 1: NFC Peer to Peer Protocol Stack versus OSI Reference Model

NFC Protocol Stack	**OSI Reference Model**
Application	Application
Logical Link Control	...
Media Acces Control	Data Link Layer
Physical	Physical

The main difference in these modes is the energy consumption of Initiator and Target. In the Active communication mode the power required for generating the RF field is shared by Initiator and Target, whereas in Passive communication mode the Initiator has to supply the power required for the field generation. To ensure proper communication, NFCIP-1 defines the following protocol flow: All devices should stay in Target mode and don't generate an RF field as default. A device switches only to Initiator mode if it is required by the application, and the application defines the use of Active or Passive communication mode. Before activating the RF field the Initiator has to check against another active sender so no other communication is disturbed. If no other RF field is detected the Initiator starts communication and tells the Target to use Active or Passive communication mode and transmission speed. After communication, both devices switch back to Target mode and deactivate their RF fields [16].

In the MAC Layer only the Initiator can start a data transmission, the LLCP enables Asynchronous Balanced Mode (ABM) where additionally the Target is able to start a data transfer and error recovery is possible. LLCP is also capable of managing multiple applications' access at the same time by multiplexing. It delivers a Connectionless Transport Protocol with a minimum of protocol overhead, for use when a higher level protocol uses flow control mechanisms. A connection-oriented transport protocol is also provided, which ensures a guaranteed and sequenced delivery of the data units. LLCP does not provide a secure data transfer mode.

B. *Reader / Writer Mode:* The tags can be placed in posters or other places and by touching the tag with the NFC device, the stored information is transmitted to the device. They can contain only information (e.g. Internet addresses) or perform actions on the device (e.g. connect to a Wireless Network). This mode is fully compatible with the ISO/IEC 14443 and FeliCa technology and because of this; NFC devices can be used as readers / writers in existing RFID infrastructures. The NFC Forum does not include Vicinity systems (ISO/IEC 15693 [16]) to the Reader / Writer Mode, but NFCIP-2 does [16].

C. *Card Emulation Mode*: The optional Card Emulation Mode allows the NFC device to communicate with well known RFID readers. The device therefore can emulate one or more RFID smartcards. With this mode it is possible to use the existing contactless infrastructure e.g. for payment or admission control. The emulation

of the smartcard can be done either in application or in a so called Secure Element. A Secure Element is a device, similar to a real smartcard but uses an interface to the NFC device to transfer its data. In combination with the Reader / Writer Mode, it is possible to implement a mode similar to the Peer to Peer Mode, but it is simpler because the protocol stack defined in Peer to Peer Mode is not needed. With the correct hardware implementation it is possible to use this mode even when the NFC device is switched off or is short of energy.

Hardware Architecture

NFC is an inductive coupled technology, the frequency of the RF field is 13.56 MHz. The specified data rates (106kBit/s, 202kBit/s and 404kBit/s) are a consequence of the compatibility with the MIFARE (ISO/IEC 14443 Type A [16]) and FeliCa (JIS X 6319-4 [35]) RFID standards.The main components of the NFC environment are[17]:
1. Host-Controller Application Execution Environment (AEE), the environment where the application rests e.g. mobile phone,
2. Secure Element Trusted Execution Environment (TEE), the secure environment where e.g. debit card data are stored,
3. NFC-ControllerContactless Front-end (CLF), the link between Host and NFC, with an interface to the Secure Element,
4. NFC-Antenna.

NFC-Controller
The NFC-Controller is the link between Air Interface, Host-Controller and Secure Element. The Host-Controller is most likely a mobile device (e.g. a mobile phone, or a smart car key [17]). Between Host- and NFC-Controller there are interfaces like Serial Peripheral Interface (SPI), Inter-Integrated Circuit (I2C) and Universal Serial Bus (USB) in use. For the communication with the Secure Element there are typically smartcard interfaces, the NFC Wired Interface or the Single Wire Protocol in use. The Controller works as modulator / demodulator between the analog Air Interface and other digital interfaces. The NFC-Controllers have integrated microcontrollers, which implement the low level services, so the exchange with the HostController is limited to the application Data and some control commands [17]. In some cases (e.g. Card Emulation Mode for payment applications with mobile phones) the NFC-Controller and the Secure Element should still work when the host is turned off or the battery is empty. For such cases, the interface between NFC Controller and Secure Element needs the possibility to power the Secure Element with the energy the NFC-Controller retrieves from the Air Interface. The NFCController can be connected to more than one Secure Element [17].

3.2.2 Secure Element
On most mobile devices (such as mobile phones) there is no way to store secure data directly. But for most NFC applications (e.g. payment and authentication solutions) such a storage system is essential. For such data, the storage needs to be secured from manipulation. Thus, it must be able to execute cryptographic functions and to implement a secure environment to execute security-relevant software. Smartcards usually implements these requirements [12].

To implement such a Secure Element, there are different possibilities, each with its own advantages and disadvantages [12]:
1. Software without secure hardware. Software is the most flexible and independent solution, but software could not be optimally secured without the hardware as there is always the possibility that the unsecured hardware is manipulated.
2. Device integrated hardware.This is the most host dependent, but most reliable solution. The Secure Element is either a part of the host or is built in as its own chip. The communication with the element and the NFC Controller works like a smartcard or over the NFC Wired Interface (see Section 1.2.3). The biggest disadvantage of this solution is, if the user changes the device, the provider of the secure service has to remove the data from the old device and to put it on the new one.
3. Changeable hardware.In most cases, this would be the best compromise between reliability, usability and costs. Because a hardware interface is needed to plug in the removable Secure Element, the production costs of the host device are higher. Such removable devices could be a Secure Memory Card (SMC), which combines the secure smartcard functions with a usual memory card function, or a Universal Integrated Circuit Card (UICC); for example in a mobile phone this is the Subscriber Identity Module (SIM) card. On actual SIM cards there is only one out of 8 connectors free for use, so the Single Wire Protocol (see Section 1.2.4) was introduced by European Telecommunication Standards Institute (ETSI). While the SMC is usually owned by the user (he can change his data by himself), the SIM card of a mobile phone is owned by the network provider (the network

provider must cooperate with the secure service provider). An NFC system implementing a Secure Element is often called shortly Secure NFC, this is misleading because only the data stored on the Secure Element is secured, not the whole NFC communication.

IV. SAFETY AND SECURITY

In the previous chapter we showed the principles of NFC. In this chapter we will discuss the safety and security measures of NFC. Safety is reliability regarding failures or an abstraction of avoidance of catastrophic consequences. Such consequences could be either physical injury of people or the damage of machinery. A quantitative definition can be given as the probability that the system will not exhibit a specified undesired behavior throughout a period of time [9]. "Functional safety is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs." [15] For a communication system, safety means that there is a guaranteed transfer of the data and given any disturbances there is a safe state where no catastrophic consequences can occur. Security is the prevention of unauthorized access and unauthorized manipulation of data. There is no quantitative definition possible. Security is categorized in three sections [13]: 1. Secrecy: the measurements to prevent data from unauthorized access, 2. Integrity: the measurements to prevent data from unauthorized changes, 3. Availability: the percentage of time for which the data is accessible. There are many ways to break the security of a system. However, in our further considerations we mainly concentrate on the risks given by the Air Interface of NFC.

4.1 Attacks on NFC systems

Figure 4 gives an overview of the possible attacks on a NFC Reader / Writer environment. In the other communication modes the situation is similar. The Air Interface is always the same and the participating NFC devices can always be manipulated either by the owner / user himself or without the owner's knowledge by a hacker. Based on the motivation these attacks can be classified in four categories [17]:

1. Spying: unauthorized access to information,

2. Deception: deceive through wrong information,

3. Denial of Service (DOS): compromise the availability of the NFC system

4. Protection of privacy."Because the attacker believes that his privacy is threatened by the RFID system, he protects himself by attacking the system.

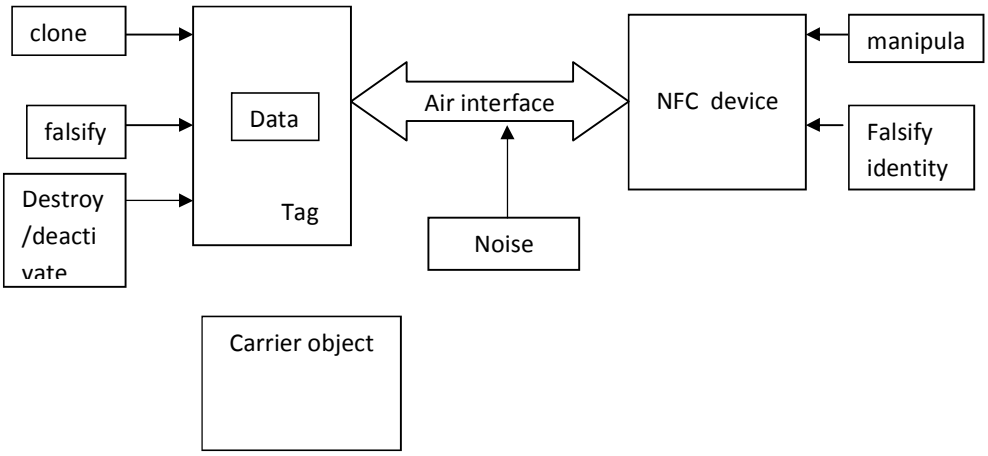

Figure 4: Schematic overview of the attacks on a NFC System

Attacks on the backend of NFC devices (e.g. a network connection to verify secure keys) would enlarge this work too much, so they are of no concern in our further discussion. For an introduction into these themes, refer to [16].

4.1.1 Attacks on the tag

The attacks which could be performed on the Tag are [5, 13, 2]:

1. Destroy: This is the simplest attack which could be used. Afterwards the tag is not able to communicate any longer with an NFC device. It could be destroyed mechanical, for example by cutting the connection to its antenna. Another way to destroy the tag is an overpowered electrical field on the tags working frequency, so that the electrical components would overload. Destroying the electrical circuits of the tag could also be done by placing the tag into a microwave oven. This attack would compromise the availability of an NFC system.

2. Remove: In this attack, the tag is removed from the carrier object. The motivation for this could be a thief, who wants to smuggle the carrier object through the security checks without recognition. This attack would compromise the availability of an NFC system.

4.1.2 Attacks over the Air Interface

Due to the fact that the Air Interface is contactless, the attacks could be performed without physical access. That means that there are many possibilities for the attacker (or his equipment) to conceal his attacks.The actual known attacks over the Air Interface are [5, 7, 13]:

1. High distance read:The attacker modifies an NFC device, to increase its range, so he can read tags from a safe distance. This is not as easy as it sounds at first. The attacker has to increase the energy of the High Frequency (HF) field, use an optimized antenna and handle the increasing noise in the communication. This attack compromises the secrecy of an NFC system.

2. Jamming:At jamming a sender blocks the NFC system by sending a disturbance signal on its frequency (13.56 MHz). This sender must be either placed near the NFC system or use appropriate antennas and power rates.This attack compromises the availability of an NFC system.

3. Denial of Service:As there could be more than one NFC device / tag in range, an anticollision algorithm has to be performed to select the individual device to communicate with. The attacker generates collisions / answers for every possible device address and simulates the existence of a high amount of devices in range of the reader. The reader will now try to reach each of the simulated devices to disable them and communicate with the desired device. But in the case that the reader can never reach the simulated devices, the desired communication is blocked. This attack compromises the availability of an NFC system.

4. Man in the Middle:In a Man in the Middle attack two parties are tricked into a three party communication, = without their knowledge. Instead of directly communication with each other they communicate through a third participant, who intercepts the messages between the other two. Thus he is able to modify data before sending it to the original receiver. An authentication system would not help, because the attacker can also intercept and set up one secure channel to the first party and a second secure channel to the second one.This attack compromises the secrecy and integrity of an NFC system.

5. Eavesdrop:Since NFC systems communicates over an open (accessible) medium (air) with electromagnetic waves, eavesdropping is a logical attack. Because the receiver of the attacker does not need the power of the active part of the communication for answering, he would be able to amplify weak signals received over a distance up to 30 -40cm [8, 10]. [10] shows that producing such a eavesdrop equipment can be done at relatively low coast. This attack would compromise the secrecy of an NFC system.

6. Relay Attack:In this attack the invader uses another communication channel (relay) as an intermediary to increase the range. The attacker needs no physical access to the device, but only an antenna and the relay in reading range. The other, perhaps more conspicuous, devices could be far away. This attack would compromise the secrecy of an NFC system.

7. Data Modification: The attacker utilizes modulation of the signal to provide the receiver a valid but manipulated message. The feasibility of this attack depends highly on the coding mechanism for the modulation, and the data can not be changed arbitrary but only to dominant states.
This attack compromises the integrity of an NFC system.

8. Data Insertion: If the answering device needs a long time for its answer, the attacker could insert a message into the communication. This would be only successful if the transmission is finished, before the answering device starts with its answer. Otherwise the message would be corrupted. This attack compromises the integrity of an NFC system.

4.1.3 Attacks on the NFC device

An NFC device could be a complex and powerful device (e.g. a mobile phone), so there is a high potential of possible attacks, for example hacking into an application which uses the NFC interface. The attacks on the NFC device could be performed either with the knowledge of the user (he is the attacker) or without the user's knowledge (e.g. a hacker accesses the device through an internet connection). At the device level nearly anything could be done to compromise the NFC system (e.g. falsify data, or gain a stolen ID). The mainly targeted classes would be integrity and secrecy but availability is also possible (e.g. the device is used to perform a DOS attack).

V. EXPERIMENTAL SETUP:

The W78E054D/W78E052D/W78E051D series contains 16K/8K/4K bytes Flash EPROM programma- ble by hardware writer; a 256 bytes RAM; four 8-bit bi-directional (P0, P1, P2, P3) and bit-addressable I/O ports; an additional 4-bit I/O port P4; three 16-bit timer/counters; a hardware watchdog timer and a serial port. These peripherals are supported by 8 sources 4-level interrupt capability. To facilitate pro- gramming and verification, the Flash EPROM inside the W78E054D/W78E052D/W78E051D series allows the program memory to be programmed and read electronically. Once the code is confirmed, the user can protect the code for security.

The W78E054D/W78E052D/W78E051D series microcontroller has two power reduction modes, idle mode and power-down mode, both of which are software selectable. The idle mode turns off the proc-essor clock but allows for continued peripheral operation. The power-down mode stops the crystal os-cillator for minimum power consumption. The external clock can be stopped at any time and in any state without affecting the processor. The W78E054D/W78E052D/W78E051D series contains In- System Programmable (ISP) 2KB LDROM for loader program, operating voltage from 3.3V to 5.5V.

Note: If the applied VDD is not stable, especially with long transition time of power on/off, it's recommended to apply an external RESET IC to the RST pin for improving the stability of system.

In the operation of the module ,the first step is to bring the RFID card near the reader ,the reader receives the unique number of the RFID card and sends it to the microcontroller , where the controller checks for the data related to the RFID number from the card , after verifying the microcontroller generate a OTP and sents a massage using a GSM module in the system to the phone no pre-registered and stored in the bank account data , on receiving the OTP the user in now authorized to access their bank account on typing the correct OTP using the keyboard

A. *A feature of microcontroller is as follows.*

• Fully static design 8-bit CMOS microcontroller • Optional 12T or 6T mode „ 12T Mode, 12 clocks per machine cycle operation (default), Speed up to 40 MHz/5V „ 6T Mode, 6 clocks per machine cycle operation set by the writer, Speed up to 20 MHz/5V • Wide supply voltage of 2.4V to 5.5V • Temperature grade is (-40oC~85oC) • Pin and Instruction-sets compatible with MCS-51 • 256 bytes of on-chip scratchpad RAM • 16K/8K/4K bytes electrically erasable/programmable Flash EPROM • 2K bytes LDROM support ISP function (Reference Application Note) • 64KB program memory address space • 64KB data memory address space • Four 8-bit bi-directional ports • 8-sources, 4-level interrupt capability • One extra 4-bit bit-addressable I/O port, additional INT2 /INT3 (available on PQFP, PLCC and LQFP package) • Three 16-bit timer/counters • One full duplex serial port • Watchdog Timer • EMI reduction mode • Software Reset • Built-in power management with idle mode and power down mode • Code protection • Packages: DIP40, PLCC44, PQFP44, LQFP48.

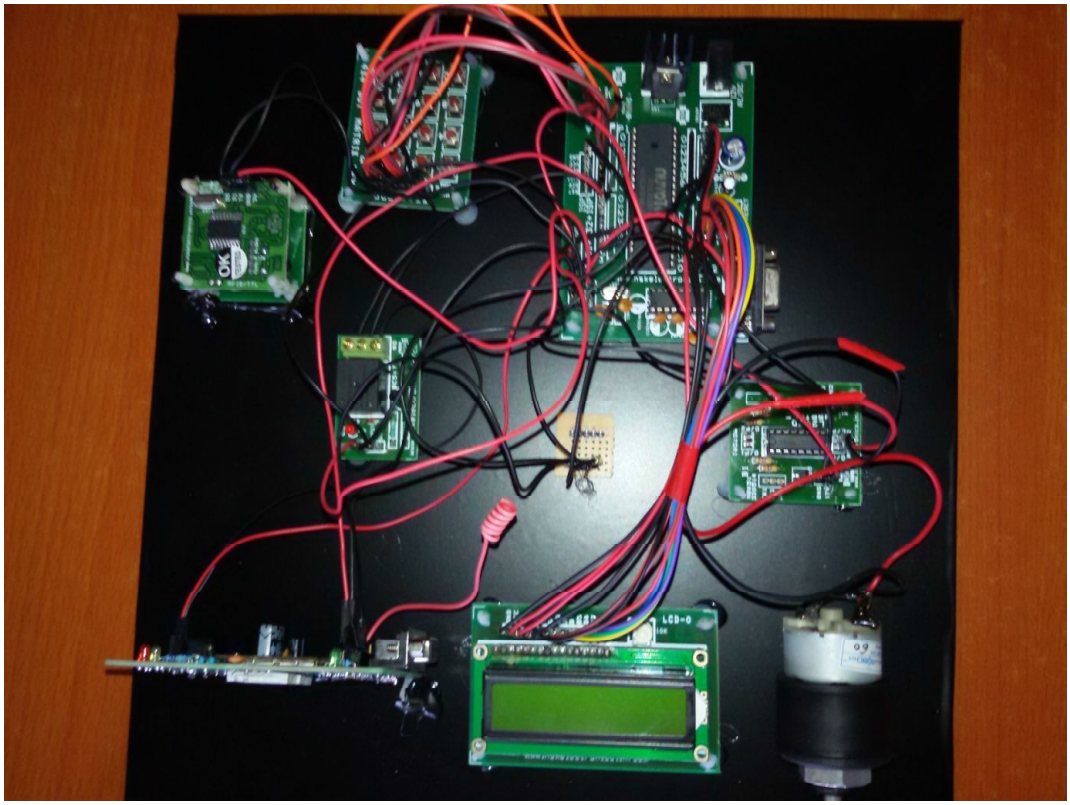

Figure 6 shows the proposed module for NFC protocol operation.

VI. CONCLUSION

Thus the above literature survey defines clearly about the existing system for we developed a proof of concept that shows, that NFC enabled devices can be connected to an existing Mobile Database. Further studies and experience will show how and if mobile consumer devices will augment daily transactions of money.

REFERENCES

[1] Jan A. Audestad. Network aspects of the GSM system. In EUROCON 88, June 1988.
[2] D. M. Balston. The pan-European system: GSM. In D. M. Balston and R.C.V. Macario, editors, Cellular Radio Systems. Artech House, Boston, 1993.
[3] David M. Balston. The pan-European cellular technology. In R.C.V. Macario, editor, Personal and Mobile Radio Systems. Peter Peregrinus, London, 1991.
[4] M. Bezler et al. GSM base station system. Electrical Communication, 2nd Quarter 1993.
[5] David Cheeseman. The pan-European cellular mobile radio system. In R.C.V. Macario, editor, Personal and Mobile Radio Systems. Peter Peregrinus, London, 1991.
[6] C. Déchaux and R. Scheller. What are GSM and DCS. Electrical Communication, 2nd Quarter 1993.
[7] M. Feldmann and J. P. Rissen. GSM network systems and overall system integration. Electrical Communication, 2nd Quarter 1993.
[8] John M. Griffiths. ISDN Explained: Worldwide Network and Applications Technology. John Wiley &Sons, Chichester, 2nd edition, 1992.
[9] I. Harris. Data in the GSM cellular network. In D. M. Balston and R.C.V. Macario, editors, Cellular Radio Systems. Artech House, Boston, 1993.
[10] I. Harris. Facsimile over cellular radio. In D. M. Balston and R.C.V. Macario, editors, Cellular Radio Systems. Artech House, Boston, 1993.
[11] Thomas Haug. Overview of the GSM project. In EUROCON 88, June 1988.
[12] Josef-Franz Huber. Advanced equipment for an advanced network. Telcom Report International, 15(3-4), 1992.
[13] Hans Lobensommer and Helmut Mahner. GSM - a European mobile radio standard for the world market. Telcom Report International, 15(3-4), 1992.
[14] Bernard J. T. Mallinder. Specification methodology applied to the GSM system. In EUROCON 88, June 1988.
[15] Seshadri Mohan and Ravi Jain. Two user location strategies for personal communication services. IEEE Personal Communications, 1(1), 1994.

[16] Lahtela, A.; Hassinen, M.; Jylha, V.; "RFID and NFC inhealthcare:Safety of hospitals medication care,"
[17] Klaus Bayrhammer, Thomas Grechenig, HaraldKöstinger, Michael Fiedler, Wolfgang Schramm__³Using a Rule-