ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

SECURE PSEUDONYM-BASED NEAR FIELD COMMUNICATION PROTOCOL FOR THE CONSUMER INTERNET OF THINGS

B.ABISHA
ME Communication Systems, Department of ECE,
Rajas Engineering College, Raja Nagar,Vadakkangulam-627 116
Tamil Nadu. India
Mobile : +919042216140
abishakrishnan02@gmail.com

T.LEENA
ASSISTANT PROFESSOR
Department of EEE
Rajas Engineering College
Vadakkangulam.
Tamil Nadu. India
Mobile : +919442364207
leenaswamy@rediffmail.com

Abstract—Near Field Communication (NFC) has been used for short range communications in a number of applications for consumer electronics devices. Specifically, NFC has been used in electronic payment systems. To ensure secure communications, security protocols for various NFC applications have been proposed. Recently, a conditional privacy preserving security protocol was introduced. However this project demonstrates that the protocol is vulnerable to two impersonations attacks and then proposes a new secure pseudonym-based NFC protocol that eliminates vulnerabilities of the previous security protocol. Security and performance analysis results confirm that the proposed protocol could solve security problems of the previously introduced NFC security protocol with a marginal computational cost increase.

I. INTRODUCTION

With the advancements in short-range wireless communication technology, the Near Field Communication (NFC) technology is being used at large scale both from academia and industry. The communication distance of the NFC technology works nearly up to 4 inches. Its operating frequency is 13.56 MHz with the transmission speed range from 106 Kbps to 424 Kbps. Various smart devices have been widely used and are also expected to be continuously used in the Internet of Things (IoT) environment. The combination of the smart devices and NFC technology expands the use of the smart devices in a number of applications, such as service discovery, e-payment, ticketing, and so on.

As an important privacy protection method, pseudonym based privacy protection methods have been widely used in many applications. In such method, the user's identity is represented by a pseudonym, which is generated by the third trusted party randomly and has no relation to the user's real identity. Therefore, the adversary cannot get the user's real identity even if he could get the user's pseudonym. In order to protect the user's privacy, Eun et al. proposed a conditional privacy preserving security protocol using pseudonyms for NFC applications. Eun et al. claimed that their protocol could withstand various types of attacks. However, this paper reveals that Eun et al.'s protocol cannot withstand impersonation attacks by providing an analysis with respect to two different types of attacks. This paper also proposes a new pseudonym based NFC protocol to secure the consumer IoT.

Objects of NFC could be divided into initiator and targetobjects. An initiator object generates a radio frequency fieldand starts the NFC interface. After receiving communicationsignals, a target object sends a response message to theinitiator object through the radio frequency field. However,due to the shared nature of wireless communication media, theNFC technology is vulnerable to many kinds of attacks.Security is thus one of the most important issues for the NFCtechnology. To enhance security, the NFC security standardshave been proposed to define data exchange format, tag types,and security protocols, e.g., a key agreement protocol forsecure NFC. For efficient key management andrevocation among nodes, i.e., initiator and target objects, aPublic Key Infrastructure (PKI) is used to build NFC securitystandards. In the PKI infrastructure, when two userswant to execute key agreement protocols, they have toexchange their certificates to get the public key of anotherparty. The certificate is generated by a Certificate Authority(CA) and the user's identity is included in it. Therefore, theadversary could track the user's action by tracing its publickey and the user's privacy may be broken.

II. LITERATURE REVIEW

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

2.1 An Anonymous Dos-Resistant Password-Based Authentication, Key Exchange and Pseudonym Delivery Protocol For Vehicular: Joseph Chee Ming Teo, Lek Heng Ngoh and Huaqun Guo Vehicular networks are gaining popularity because vehicular communications are able to help minimize accidents, improve traffic conditions and provide infotainment services. Security and privacy are important challenges in the deployment of vehicular networks. Authentication key exchange and pseudonym delivery protocols can be used to provide security and privacy in vehicular networks. However, two important aspects of security and privacy, namely protection against DoS attacks and vehicle node anonymity, are currently not being addressed in existing authentication, key exchange and pseudonym delivery protocols for vehicular networks. In this project, we propose an anonymous DoS-resistant password based Authentication Key Exchange and Pseudonym delivery (AUCKEPER) protocol for vehicular networks that provides both protections against DoS attacks and vehicle node anonymity. A security and complexity analysis shows that the proposed AUCKEPER protocol is secure, more efficient and has advantages over a recently proposed state-of-the art authentication, key exchange and pseudonym protocol.Password-based mechanism has been the most widely used method for user authentication since it allows people to choose and remember their own passwords without any assistant device. However, human users usually choose easy-to-remember passwords so that they are vulnerable to password guessing attacks. On the contrary, the entities excluding human users, such as servers, can directly use strong cryptographic secrets for entity authentication and hence prevent password guessing attacks. This model consists of two servers with a client. To distinguish this with the existing model, we call this a client–server–server model. In this environment, a workstation cannot be trusted to identify its users correctly to network services.

2.2 Strong and Affordable Location Privacy In Vanets: Identify Diffusion Using Time Slots And Swapping: David Eckhoff, Christoph Sommer, Tobias Ganseny, Reinhard German and Falko Dressler.

Public acceptance, and thus the economical success of Vehicular Ad Hoc Networks (VANETs), is highly dependent on the quality of deployed privacy mechanisms. Neither users nor operators should be able to track a given individual. One approach to facilitate this is the usage of pseudonym pools, which allow vehicles to autonomously switch between different identities. We extend this scheme with that of a time-slotted pseudonym pool of static size, reducing the storage and computation needs of the envisioned Intelligent Transportation System (ITS) while further improving users' privacy. In addition, we allow the exchange of pseudonyms between nodes, eliminating the mapping between vehicles and pseudonyms even for operators of the VANET. Here, we support the exchange of both the currently used pseudonym and those of future time-slots, further enhancing users' privacy. We evaluate the feasibility of our approach and back up privacy claims by performing a simulative study of the system using the entropy of nodes' anonymity sets as the primary metric.Vehicular Ad Hoc Networks (VANETs) are created by applying the principles of mobile ad hoc networks (MANETs) - the spontaneous creation of a wireless network for data exchange - to the domain of vehicles. They are a key component of intelligent transportation systems (ITS).Intelligent Transportation Systems (ITSs) offer a wide range of services based on wireless communication. Many of these, such as location-based services or driving assistance, require the exchange of positions and identifiers of cars in the vicinity to operate. A commonly used method in VANET is that vehicles send periodic beacon messages to inform other entities about their current state and position. An adversary is thus able to track a single entity throughout the system just by overhearing communication, collecting and then aggregating this data This can severely compromise the privacy of users, because a car is usually only driven by very few different drivers. However, even if the location is not included in these messages, the position of a sending node can be determined with sufficient precision by other vehicles and Roadside Units (RSUs), using triangulation or simple range estimations. This allows an operator or any other user to create accurate traces of all participants if the number of observations is high enough.

2.3ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications: Rongxing Lu, Xiaodong Lin, Haojin Zhu, Pin-Han Ho and Xuemin (Sherman) Shen.

Efficient conditional privacy preservation (ECPP) protocol in vehicular ad-hoc (VANETs) is to address the issue on anonymous authentication for safety messages with authority traceability. The proposed protocol is characterized by the generation of on-the-fly short-time anonymous keys between on-board units (OBUs) and roadside units (RSUs), which can provide fast anonymous authentication and privacy tracking while minimizing the required storage for short-time anonymous keys. We demonstrate the merits gained by the proposed protocol through extensive analysis.The increasing demand for improving road safety and optimizing road traffic has brought a

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

wide interest on vehicular ad hoc networks (VANETs). As a special instantiation of mobile ad-hoc networks (MANETs), VANETs have been positioned to serve as a general platform for the future development of vehicular-centered applications which require local data collection and generation via local information, data floating and information distribution through both point-to-multipoint and peer-to-peer fashions. A VANET mainly consists of On-Board Units (OBUs) and Roadside Units (RSUs), where OBUs are installed on vehicles to provide wireless communication capability, while RSUs are deployed to provide wireless interfaces to vehicles within their radio Coverage's.Extensive research efforts have been made by both industry and academia to investigate some key issues in vehicular networks, where security assurance and privacy preservation are two primary concerns. Without the security and privacy guarantee, serious attacks may jeopardize the benefits by the improved driving safety since an attacker could track the locations of the interested OBUs and obtain their moving patterns. Therefore, how to provide anonymous safety message authentication has become a fundamental design requirement in securing vehicular networks. However, anonymous message authentication in vehicular networks is a double-edge sword. A well-behaved OBU, due to the privacy protection mechanism, is willing to offer as much local information as possible to its neighboring OBUs and RSUs to create a safer and more efficient driving environment. However, a maliciously-behaved OBU may abuse the privacy protection mechanism by damaging the regular driving environment. This particularly happens when a driver who is involved in a dispute event of safety messages may intend to escape from the investigation and responsibility. Therefore, the anonymous message authentication in vehicular networks should be conditional, such that a trusted authority can find a way to track a targeted OBU and collect the safety messages it has disseminated, even though the OBU is not traceable by the public.

2.4 PACP: An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for Vanets: Dijiang Huang, Satyajayant Misra, Mayank Verma, and Guoliang Xue.

Anew privacy preservation scheme, named pseudonymous authentication-based conditional privacy (PACP), which allows vehicles in a vehicular ad hoc network (VANET) to use pseudonyms instead of their true identity to obtain provably good privacy. In our scheme, vehicles interact with roadside units to help them generate pseudonyms for anonymous communication. In our setup, the pseudonyms are only known to the vehicles but have no other entities in the network. In addition, our scheme provides an efficient revocation mechanism that allows vehicles to be identified and revoked from the network if needed. Thus, we provide conditional privacy to the vehicles in the system, that is, the vehicles will be anonymous in the network until they are revoked, at which point, they cease to be anonymous.Vehicular ad hoc networks (VANETs) have recently become a popular direction for research, with specific attention to improving driving experience and road safety. VANETs generally consist of vehicles, infrastructure units such as roadside units (RSUs), and a centralized trusted authority. Each vehicle that is part of a VANET contains an onboard wireless computing unit, which is commonly known as the onboard unit (OBU). Vehicles may communicate with the RSUs, which are online, and with other vehicles in their neighborhood. Recent studies on VANETs have identified several issues, including those in security and privacy, which need to be addressed for widespread adoption. Security issues in VANETs have been studied in great detail. However, the issue of privacy still has a lot of open questions. With the latest advancement in tracking mechanisms and the potential increase in communication among vehicles, an adversary can track a vehicle by observing its communication and movement patterns. However, if a completely anonymized vehicle turns malicious, then there is no way to identify and revoke it.

2.5 Conditional Privacy Preserving Security Protocol for NFC Applications: Hasoo Eun, Hoonjung Lee, and Heekuck Oh.

Recently, various mobile terminals equipped with NFC are released. However, The NFC security standard currently applied uses the user's public key constantly in the process of key agreement. Since it does not provide with unlinkability between user messages, privacy infringement may happen. This project proposes a method provide a conditional anonymity using dynamic public key to solve this problem. Also it defines PDU for the conditional anonymity, so that the user can use the dynamic public key selectively. Through this, the user can protect privacy and can verify identity through a trusted authority if necessary. NFC (Near field Communication) is a short-range wireless communication technology whose 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. To use NFC in electronic payment, security is a prerequisite to be addressed. The

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

public key is received from CA (Certificate Authority), and it uses a fixed value until reissued.

2.6 Anonymous Two-Factor Authentication for Consumer Roaming Service in Global Mobility Networks: Debiao He, Neeraj Kumar, Muhammad K. Khan, Jong-Hyouk Lee.

As a mechanism to secure access to a global mobility network (GLOMONET), authentication for consumer roaming service is an essential technology. Moreover, as mobile consumers are getting concerned about how much information network providers gather about them, privacy preservation is a serious concern these days. In this project, a new authentication scheme is presented that provides a robust anonymous two-factor authentication for consumer roaming service in GLOMONETs. Detailed operational phases of the proposed scheme are provided. Security analysis is provided to confirm that the proposed scheme provides anonymity, authentication, and perfect forward secrecy. In addition, the proposed scheme is analyzed whether it withstands various attacks.Global Mobility Networks (GLOMONETs) have become widely available and interconnected. To provide global roaming service for a mobile user, remote authentication is an essential requirement. A typical remote authentication scenario involves three parties, namely a Mobile User (MU), a Foreign Agent (FA) and a Home Agent (HA). When a mobile user MU roams into a foreign network, the foreign agent FA authenticates the roaming user with the help of the user's home agent HA.During the roaming process in GLOMONET, the mobile user MU is very much concerned about its privacy protection. The user's identity should be protected and his/her location and activities should be kept unlinkable. It is desirable to keep mobile users' identities anonymous in the remote user authentication process. In recent years, many anonymous authentication scheme have been proposed for roaming services in GLOMONET. However, most of the existing protocols were broken shortly after they were proposed.

2.7 Robust Biometrics-Based Authentication Scheme for Multiserver Environment: Debiao He, and Ding Wang

The authentication scheme is an important cryptographic mechanism, through which two communication parties could authenticate each other in the open network environment. To satisfy the requirement of practical applications, many authentication schemes using passwords and smart cards have been proposed. However, passwords might be divulged or forgotten, and smart cards might be shared, lost, or stolen. In contrast, biometric methods, such as fingerprints or iris scans, have no such drawbacks. Therefore, biometrics-based authentication schemes gain wide attention. In this project, we propose a biometrics-based authentication scheme for multiserver environment using elliptic curve cryptography. To the best of our knowledge, the proposed scheme is the first truly three-factor authenticated scheme for multiserver environment. We also demonstrate the completeness of the proposed scheme using the Burrows–Abadi–Needham logic.Given biometric input B, a fuzzy extractor could extract a random string σ. One important property of the fuzzy extractor is that it could output the same random string when the input changes, but it remains close. Gen is a probabilistic generation procedure. Upon receiving biometric input B, the procedure will output a random string σ and a random auxiliary string ν. Rep is a deterministic reproduction procedure. Upon receiving a close biometric input $B^*$and the corresponding random auxiliary string ν, the procedure will recover σ.We call a fuzzy extractor is secure if it is difficult to recover σ from a closed biometric input B^*without the auxiliary string ν.

2.8 Enhanced Three-Factor Security Protocolfor Consumer USB Mass Storage Devices: Debiao He, Neeraj Kumar, Jong-Hyouk Lee, and R. Simon Sherratt.

The Universal Serial Bus (USB) is an extremely popular interface standard for computer peripheral connections and is widely used in consumer Mass Storage Devices (MSDs). While current consumer USB MSDs provide relatively high transmission speed and are convenient to carry, the use of USB MSDs has been prohibited in many commercial and everyday environments primarily due to security concerns. Security protocols have been previously proposed and a recent approach for the USB MSDs is to utilize multi-factor authentication. This project proposes significant enhancements to the three-factor control protocol that now makes it secure under many types of attacks including the password guessing attack, the denial-of-service attack, and the replay attack. The proposed solution is presented with a rigorous security analysis and practical computational cost analysis to demonstrate the usefulness of this new security protocol for consumer USB MSDs. In Lee *et al.'s* three-factor authentication protocol U inserts their storage device into a client terminal and inputs their password, identity and biometric signature. Mutual authentication is then executed between U and AS. U obtains a session key from AS if they are successfully authenticated. With this key, U can store an encrypted file on the storage device.When U is successfully authenticated, a shared session key is generated between U and AS. Then, the session key will be used to encrypt the files transferred via the USB interface. When U decrypts the files on the

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

storage devices, *U* must do the same authentication and generate the same session key for the original file. Every filename and user's identity will have a session key and different files or users' identity have different session keys. To ensure system security, the temporarily stored session key will be deleted after encrypting or decrypting the file. Lee *et al.*'s protocol has the following three characteristics: only authorized users can access the USB consumer storage devices; files taken from the storage devices cannot be decrypted without the session key; and other legal users cannot decrypt a legal classified file even if it is copied to their storage device. Therefore the original file is secure.

III. PROPOSED SYSTEM

Near field communication (NFC) is the set of protocols that enable electronic devices to establish radio communication with each other by touching the devices together, or bringing them into proximity to a distance of AVRally 10cm or less.

Early business models such as advertising and industrial applications were not successful, having been overtaken by alternative technologies such as bar codes or UHF tags, but what distinguishes NFC is that devices are often cloud connected. All NFC-enabled smart phone can be provided with dedicated apps including 'ticket' readers as opposed to the traditional dedicated infrastructure that specifies a particular standard for stock ticket, access control and payment readers. By contrast all NFC peers can connect to a third party NFC device that acts as a server for any action.

NFC tag is given as the input and NFC tag can be read by an NFC card reader. It is supported by a microcontroller, keypad is used to type the necessary data's, and an LCD is used for display and GSM for sending the data to the mobile phone. The communication distance of the NFC technology works nearly up to 4 inches. Its operating frequency is 13.56 MHz with the transmission speed range from 106 Kbps to 424 Kbps. The combination of the smart devices and NFC technology expands the use of the smart devices in a number of applications.

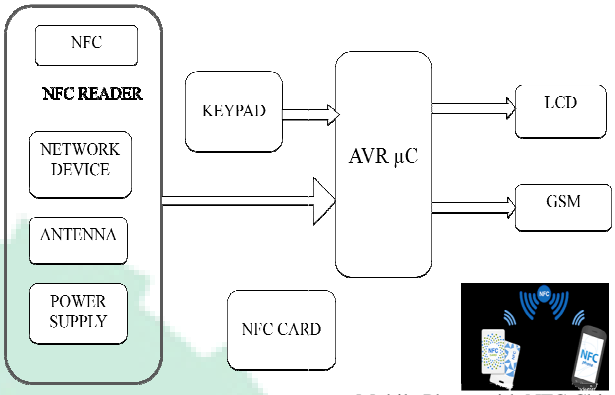

Fig1. Proposed Block Diagram

NFC card/tag is a near field communication card used in different applications. NFC Card emulation mode enables NFC-enabled devices such as smart phone to act like smart cards, allowing users to perform transactions such as payment or ticketing..A near field communication tag is a sticker or wristband with small microchips that can be read by in range mobile devices. Information is stored in these microchips. Many of today's smart phones have built-in NFC capabilities, and smart phone users can purchase and acquire tags online. The amount of information stored on a NFC tag depends on the tag type, as tag memory capacity varies by tag. For example, a tag can store a phone number or URL.A modern example of a commonly used NFC tag function is mobile payment processing, where users swipe or flick a mobile phone on a NFC reader. Google's version of this system is Google Wallet.

A NFC tag has the ability to send data to other mobile phones with NFC capabilities. NFC tags also perform a variety of actions, such as changing handset settings or launching a website.NFC, or near-field communication**,** is an easy and intuitive technology that allows you to use your mobile phone for special purposes. An NFC tag can share and link to information such as web pages, social media and all other sorts of other information generally. Other areas where NFC is starting to evolve into are making payments, opening doors secured with contactless locks, logging on to computers and many more. All of these actions have something in common, that is they invoke an action based on you placing your phone near the thing you want to read or interact.

3.1 GSM

GSM, is a standard developed by the European Telecommunications Standards Institute (ETSI) to

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

describe the protocols for second-generation (2G) digital cellular networks used by mobile phones.

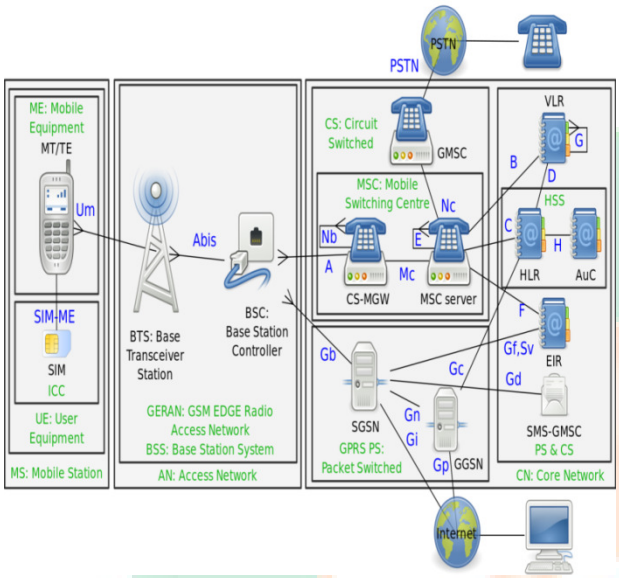

Fig 2 Structure of a GSM Network

GSM is a cellular network, which means that cell phones connect to it by searching for cells in the immediate vicinity. The user cannot confirm the real identity of another party. Based on the observation, we thus propose the following two impersonation attacks against their protocol. There are five different cell sizes in a GSM network—macro, micro, pico, femto, and umbrella cells. The coverage area of each cell varies according to the implementation environment. Macro cells can be regarded as cells where the base stationantenna is installed on a mast or a building above average rooftop level. Micro cells are cells whose antenna height is under average rooftop level; they are typically used in urban areas. Pico cells are small cells whose coverage diameter is a few dozen meters; they are mainly used indoors. Femto cells are cells designed for use in residential or small business environments and connect to the service provider's network via a broadband internet connection. Umbrella cells are used to cover shadowed regions of smaller cells and fill in gaps in coverage between those cells.

3.2 WORKING PRINCIPLE

The Block diagram consists of mobile phone, LCD, NFC card, microcontroller, NFC reader. NFC tag is given as the input and NFC tag can be read by an NFC card reader.

It is supported by a microcontroller, keypad is used to type the necessary data's, an LCD is used for display and GSM is for sending the data to the mobile phone. In the proposed system security can be enhanced by a pseudonym based privacy protection methods have been widely used in many applications.

In such method, the user's identity is represented by a pseudonym, which is generated by the third trusted party randomly and has no relation to the user's real identity. Therefore, the adversary cannot get the user's real identity even if he could get the user's pseudonym in order to protect the user's privacy.

NFC tag is given as the input and NFC tag can be read by an NFC card reader. It is supported by a microcontroller, keypad is used to type the necessary data's, and an LCD is used for display and GSM for sending the data to the mobile phone. The communication distance of the NFC technology works nearly up to 4 inches. Its operating frequency is 13.56 MHz with the transmission speed range from 106 Kbps to 424 Kbps. The combination of the smart devices and NFC technology expands the use of the smart devices in a number of applications.

3.3 NEAR FIELD COMMUNICATION

NFC, or near-field communication, is an easy and intuitive technology that allows you to use your mobile phone for special purposes. An NFC tag can share and link to information such as web pages, social media and all other sorts of other information generally. Other areas where NFC is starting to evolve into are making payments, opening doors secured with contactless locks, logging on to computers and many more. To enhance security, the NFC security standards have been proposed to define data exchange format, tag types, and security protocols. All of these actions have something in common, that is they invoke an action based on you placing your phone near the thing you want to read or interact with.

Reader/Writer and Card

TV AVRally a transaction occurs between an active device that sends out signals and receives information and a passive device that simply sends the information and does not receive anything other than instructions on what data to reply with. The reader/writer is the Smartphone serving as the active device and the card is the NFC tag serving as the passive device. Smart phone can take on the role of card, however, when they act as a credit card for contactless payments. Then the credit card reader becomes the reader/writer and the Smartphone serves as the passive card device.

Initiator and Target

NFC technology has a major advantage over other technologies such as RFID. NFC can create peer-to-peer sharing between two phones. In this case, the phone making the connection or sending an invitation is the

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

initiator and the phone receiving the instructions and sending back information is the target. Yet both phones can serve both roles by switching back and forth depending on what transmission is being sent, though this requires a higher level of technology.

NFC has evolved from Radio Frequency Identification also known as (RFID). This allows a reader to send radio waves to an electronic tag for identification, authentication and tracking.

IV. RESULT AND DISCUSSION

In NFC, the object of communication is divided into an initiator and a target. An initiator generates RF field (Radio Frequency field) and starts NFCIP-1. A target that receives signals from initiator responds to the initiator through the RF field. When target communicates using RF field of initiator, it is called passive communication mode, and using self generated RF field is referred to as active communication mode. Communication mode is determined according to applications when transaction starts. Once the transaction is started, the communication mode cannot be changed until the target becomes disabled or removed.

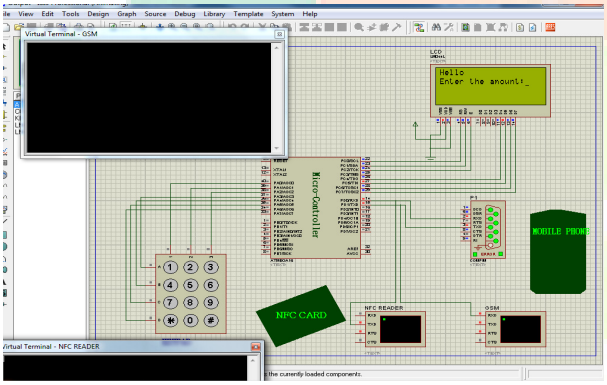

Fig 3. System design.

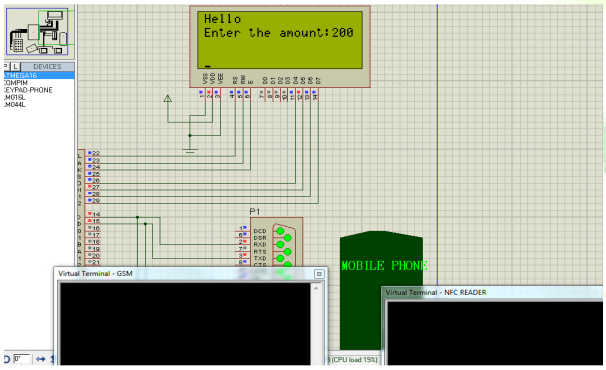

Fig 4.NFC processing

NFC-SEC defines SSE (Shared Secret service) and SCH (Secure Channel service) for NFCIP-1. SSE generates a secret key for secure communication between NFC devices and in this process, key agreement and key confirmation is performed. SCH service provides the communication between NFC devices with confidentiality and integrity using a key generated through SSE service.

1) NFC reader is used to read the NFC card which is brought near to it.
2) The amount which is used for shopping is to entered via keypad.

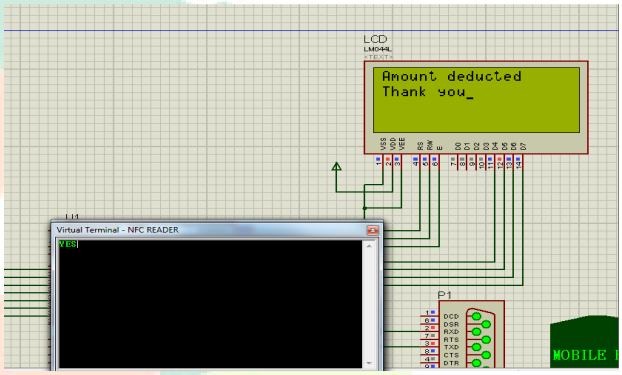

Fig 5.Representation of amount using NFC.

To have a safe shopping

1) At the time shopping the amount wgich has to be deducted is entered and it is confirmed by the user
2) Now the amount is deducted from the user account.
3) The protocol enabled the safe shooping, it avoid the hjackers etc..

V. CONCLUSION

In the IoT environment, various types of intelligent devices will communicate with one another for data collection and processing and this phenomenon will lead to the increased NFC use. Here, the recent NFC security protocol, has been analyzed. As revealed, the protocol cannot withstand the two different impersonation attacks. To address the problems, we are introducing the new secure pseudonym-based NFC protocol. A detailed analysis of the proposed scheme with respect to various types of attacks has been demonstrated that shows the proposed protocol solves the security problems while providing stronger protections to NFC.

REFERENCES

1. S. Chatterjee, A. K. Das and J. K. Sing, “An Enhanced Access Control Scheme in Wireless Sensor Networks,” *Ad Hoc & Sensor Wireless Networks*, Vol. 21, No. 1-2, pp. 121-149, 2014.
2. D. Eckhoff, C. Sommer, T. Gansen, R. German, and F. Dressler, "Strong and affordable location

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

privacy in VANETs: Identity diffusion using time-slots and swapping," *Proceedings of the 2010 IEEE Vehicular Networking Conference* (VNC 2010), pp. 174-181, Dec. 2010.

3. H. Eun, H. Lee, H. Oh, Conditional privacy preserving security protocol for NFC applications, *IEEE Trans. Consum. Electron.*,, vol. 59, no. 1, pp.153-160, 2013.
4. D. He, N. Kumar and J.-H. Lee, "Anonymous two-factor authentication for consumer roaming service in Global Mobility Networks," *IEEE Trans. Consum. Electron.*, vol. 59, no. 4, pp. 811-817, 2013.
5. D. He, N. Kumar, J.-H. Lee, R. Sherratt, "Enhanced Three-factor Security Protocol for USB Consumer Storage Devices, " *IEEE Trans. Consum. Electron.*, vol. 60, no. 1, pp. 30-37, 2014.
6. D. He and D. Wang, "Robust biometrics-based authentication scheme for multi-server environment," *IEEE Systems Journal*, DOI: 10.1109/JSYST.2014.2301517, 2014.
7. D. He, S. Wu, "Security flaws in a smart card based authentication scheme for multi-server environment," *Wireless Personal Communications*, vol. 70, no. 1, pp. 323-329, 2013.
8. D. Huang, S. Misra, M. Verma, and G.Xue, "PACP: An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs," *IEEE Transactions on Intelligent Transportation Systems*, Vol. 12, No. 3, pp. 736-746, Sept. 2011.
9. R. Lu, X. Lin, H. Zhu, P.H. Ho, and X. Shen, "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications," *Proceedings of The27th Conference on Computer Communications* (INFOCOM 2008), pp. 1229-1237, Apr. 2008.