PRIVACY PRESERVING BILLING FOR E-SHOPPING IN ONLINE MARKETING SYSTEM

R.Gayathri [1] M.Iswarya [2] D.Karthika [3] S.Selvakanmani [4]

[1,2,3,4]Department of Computer Science & Engineering
[1,2,3,4]Velammal Institute of Technology

Abstract—several daily life applications such as payment, access control, ticketing, and e-passport, which requires strong security and privacy mechanisms. Hence there is a demanding urge to address these issues in the light of some mechanism which can make the technology excel. . In recent years, various mobile terminals equipped with NFC (Near Field Communication) have been released. The combination of NFC with smart devices has led to widening the utilization range of NFC. It is expected to replace credit cards in electronic payment, especially. In this regard, security issues need to be addressed to vitalize NFC electronic payment. The NFC security standards currently being applied require the use of user's public key at a fixed value in the process of key agreement. For key agreement NFC algorithm is used. This paper 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.

*Keywords:*Near Field Communication, Protocol Data Unit, Certificate Authority Security Council, Trusted Third Party, Shared Secret service, Secure Channel service, Advanced Encryption Standard.

I. INTRODUCTION

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 [1]-[3]. Since it does not provide with unlink ability between users messages, privacy infringement may happen. This paper 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.

Various mobile terminals equipped with NFC (Near Field Communication) have been released. The combination of NFC with smart devices has led to widening the utilization range of NFC. It is expected to replace credit cards in electronic payment, especially. In this regard, security issues need to be addressed to vitalize NFC electronic payment. The NFC security standards currently being applied require the use of user's public key at a fixed value in the process of key agreement. The relevance of the message occurs in the fixed elements such as the public key of NFC. An attacker can create a profile based on user's public key by collecting the associated messages. Through the created profile, users can be exposed and their privacy can be compromised. We propose conditional privacy protection methods based on pseudonyms to solve these problems. In addition, PDU (Protocol Data Unit) for conditional privacy is defined. Users can inform the other party that they will communicate according to the protocol proposed in this paper by sending the conditional privacy preserved PDU through NFC terminals.

II. RELATED WORKS

Raja Naeem Akram, Konstantinos Markantonakis, and Keith Mayes, in the smart card industry, the application acquisition process involves the card issuers and application providers. During this process, the respective card issuer reveals the identity of the smart card user to the individual application providers. In certain application scenarios it might be necessary (e.g. banking and identity applications). However, with introduction of the Trusted Service Manager (TSM) architecture there might be valid cases where revealing the card user's identity is not necessary. At the moment, the secure channel protocols for traditional smart card architecture including the TSM do not preserve the privacy of the card users.

Hu Xiong, Jianbin Hu, Tao Yang, Wei Xin, Zhong Chen, In this introduction of an efficient and trustworthy conditional privacy-preserving communication protocol for VANETs based on proxy re-signature. The proposed protocol is characterized by the Trusted Authority (TA) designating the Roadside Units (RSUs) to translate signatures computed by the On-Board Units (OBUs) into one that are valid with respect to TA's public key. In addition, the proposed protocol offers both a priori and a posteriori countermeasures: it can not only provide fast anonymous authentication and privacy tracking, but guarantees message trustworthiness for vehicle-to-vehicle (V2V) communications. Furthermore, it reduces the communication overhead and offers fast message authentication and, low storage requirements. We use extensive analysis to demonstrate the merits of the proposed protocol and to contrast it with previously proposed solutions.

Mike Burmester, Emmanouil Magkos, and Vassilis Chrissikopoulos,in this paper we consider the problem of privacy and security in vehicular (V2V) communication, in particular securing routine safety messages. Traditional public key mechanisms are not appropriate for such applications because of the large number of safety messages that have to be transmitted by each vehicle, typically one message every 100−300ms. We first show that a recently proposed V2V communication scheme, TSVC, based on the Time Efficient Stream Loss-tolerant Authentication (TESLA) scheme is subject to an impersonation attack in which the adversary can distribute misleading safety information to vehicles, and propose a modification that

secures it against such attacks. We then address general concerns regarding the inappropriateness of TESLA for vehicular applications (caused by the delayed authentication, and buffer overflow issues), and propose a V2V communication scheme based on a variant of TESLA, TESLA0, in which packets are self-authenticating. This scheme is appropriate for applications in which vehicles are in close proximity. Finally we consider a hybrid protocol that combines both schemes and addresses in a more flexible way the mobility requirements of V2V communications.

A. Chandrasekhar, V.R. Rajasekar and V.Vasudevan, the Elliptic Curve Cryptosystem (ECC) is an emerging alternative for traditional Public-Key Cryptosystem like RSA, DSA and DH. It provides the highest strength-per-bit of any cryptosystem known today with smaller key sizes resulting in faster computations, lower power consumption and memory. It also provides a methodology for obtaining high-speed, efficient and scalable implementation of protocols for authentication and key agreement. This paper provides an introduction to Elliptic Curves and how they are used to create a secure and powerful cryptosystem. It provides an overview of the three hard mathematical problems that provide the basis for the security of public key cryptosystems used today: the Integer Factorization Problem (IFP), the Discrete Logarithm Problem (DLP), and the Elliptic Curve Discrete Logarithm Problem (ECDLP). It explains the proposed protocol which is improved to reduce the storage requirements for establishing a shared secret key between two parties, to sign and verify a document and to establish a mutual authentication between two parties. The result of implementation is also discussed.

Jieun Yu and Wonjun Lee, GENTLE: Reducing Reader Collision in Mobile RFID Networks, Mobile RFID, the technology of a cellular phone equipped with a RFID reader, allows users to read RFID tags anywhere. However, signals from more than two readers can interfere with one another, i.e. reader collision problem; reliable tag reading is necessary. Here Gentle protocol is used to send beacon messages and multi-channel for increasing throughput. In addition, Gentle protocol can put tag ID information into the beacon message and share it among close readers. Simulation results show that Gentle protocol outperforms existing reader anti-collision protocols. The RFID system consists of Radio Frequency (RF) readers and tags. In Mobile RFID, the reader is installed in the cellular phone and the services are provided over a telecommunication network. The basic idea is that readers avoid multiple reader-to-tag collision by using beacon messages when they are close one another and reader-to-reader collision by using multi-channel when the distance between those readers is long. Gentle protocol can avoid two kinds of reader collision efficiently and take advantage of given RFID multichannel resource as well as increase read throughput.

III. ARCHITECTURE DIAGRAM

In existing system, the application acquisition process involves the card issuers and application providers. During this process, the respective card issuer reveals the identity of the smart card user to the individual application providers. In certain application scenarios it might be necessary (e.g. banking and identity applications). However, with introduction of the Trusted Service Manager (TSM) architecture there might be valid cases where revealing the card user's identity is not necessary.

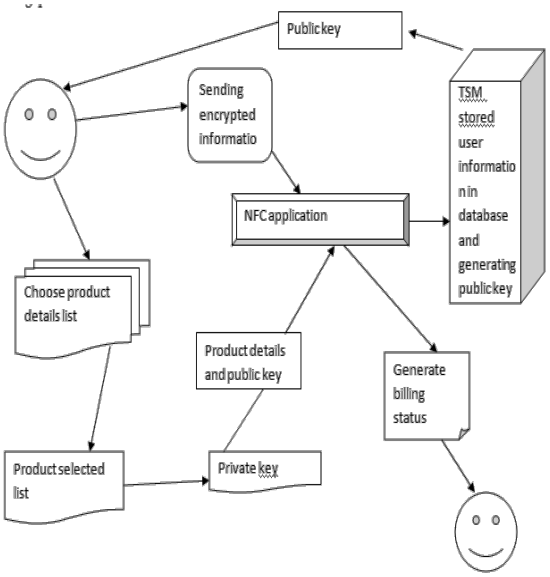

Fig. 1: Architecture Diagram of Privacy Preserving Billing for E-Shopping in Online Marketing System

At the moment, the secure channel protocols for traditional smart card architecture including the TSM do not preserve the privacy of the card users. The Near Field Communication (NFC) technology and commercial realities have reinvigorated the multi-application smart card initiative. In most of the trials, either the traditional ownership model termed as Issuer Centric Smart Card Ownership Model (ICOM) or an extension of it referred to as Trusted Service Manager (TSM) is deployed. We propose privacy protection methods based on pseudonyms to protect privacy of users. The proposed methods provide conditional privacy in which the identity of users can be verified by the TTP (Trusted Third Party) to resolve disputes when necessary. In addition, the PDU (Protocol Data Unit) for the conditional privacy is proposed in this paper. The data used to help a future purchase uses protected PDU of NFC-SEC, and data not wanted to be recorded uses conditional privacy PDU selectively, which makes it possible to remove the connectivity with the existing messages. This paper is the extended version of. It covers background, security requirements, and differences between pseudonym-based method and the proposed method.

According to survey conducted so far, this paper has its significance in the sense it is the first research on the conditional privacy protection of users in NFC.

IV. IMPLEMENTATION DESIGNS

1) User Interface Design
2) Trusted Service Manager
3) Shared Security Services
4) Security Requirement
5) Conditional Privacy Protocol Data Unit

1) USER INTERFACE DESIGN

In this module user has to create an account for only allowing right persons to access the resources. All the

details will be stored in database which is placed in server. If he entered correct user name and password then he will be able to access the public cloud.Logging in is usually used to enter a specific page, which trespassers cannot see. Once the user is logged in, the login token may be used to track what actions the user has taken while connected to the site. Logging out may be performed explicitly by the user taking some action, such as entering the appropriate command, or clicking a website link labeled as such. It can also be done implicitly, such as by the user powering off his or her workstation, closing a web browser window, leaving a website, or not refreshing a webpage within a defined period.In the case of web sites that use cookies to track sessions, when the user logs out, session-only cookies from that site will usually be deleted from the user's computer. In addition, the server invalidates any associations with the session, making any session-handle in the user's cookie store useless.

2) TRUSTED SERVICE MANAGER

In this module, two users can get a shared secret value z by taking x coordinate value at point P. When compared with the existing protocols based on the above process, Q'A and Q'B can replace QA and QB, the existing public keys. In other words, the anonymity of users can be guaranteed by replacing the public key alone, while retaining the existing protocols. This method cannot be used to specify the owner of the public key, but it can identify whether the public key is regularly generated or not. Therefore, it can be identified that the message is generated by using the public key received from TSM. In case the user's public key doesn't pass the verification, the NFC communication is discontinued. When the protocol is discontinued in the process of one-to-one short range communication, users suspect the involvement of attackers, and they can discontinue or restart the communication.

3) SHARED SECURITY SERVICES

In order to preserve privacy, one would like to do things when nobody else could see or disturb him or her. In case of NFC which can be used in overall life, an attacker can infringe the privacy of users easily by tracking usage history. Suppose that user 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 may help her to efficiently purchase products; however, it may contain information which she does not want others to know such as her health conditions or security questions.

4) SECURITY REQUIREMENTS

There are two features provided in this stage. They are:

a) Data Confidentiality
b) Data Integrity

a) Data Confidentiality

Service provides the communication between NFC application with confidentiality and integrity using a key generated through SSE (security element) service. The key generated through SSE and provides confidentiality and integrity to the messages using generated keys. The three keys created in SCH are used to provide the confidentiality and integrity of the message.

b) Data Integrity

The transmitted data should be identical to the source data. It is guaranteed that data is not modulated in the process of transferring user's purchase information PA (public key of user's).

5) CONDITIONAL PRIVACY PROTOCOL DATA UNIT

The methods proposed in this paper allow users to hide their information. However, in case information is hidden in all situations, there arises a problem where the personalized service is not provided. Therefore, additional instruction is needed so that the methods proposed in this paper can be used selectively. In this module, Users can request services through protected PDU if they want to receive the personalized service, while protecting their data from third-party attackers and through conditional privacy PDU if they want to be guaranteedto receive the conditional privacy additionally. For instance, if users want to receive the personalized services such as product recommendations, they need to use the protected PDU. When the users want to hide purchase information they need to use the conditional privacy PDU.

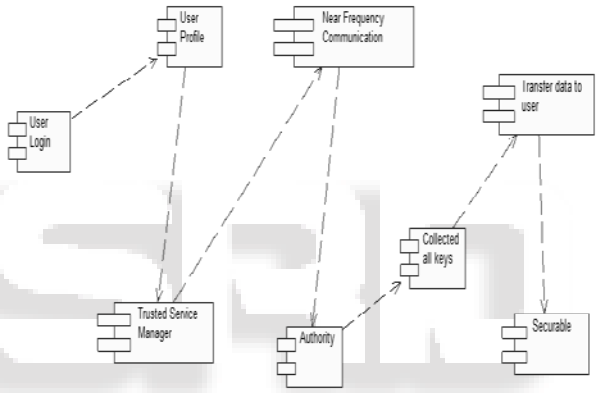

Fig. 2: Component Diagram for the process of E-Shopping

V. ALGORITHM

The algorithm used here is Advanced Encryption Standard (AES). The Advanced Encryption Standard is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.AES is based on the Rijndael cipher developed by two Belgian cryptographers, Joan Daemon and Vincent Rijmen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes. It supersedes the Data Encryption Standard (DES), which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. AES is based on a design principle known as a substitution- permutation network, and is fast in both software and hardware. AES has a different fixed block size of 8, 64,128 and key bits of 128,192,256 bits. AES operates on a 4x4 column- major order matrix of bytes, termed the state. The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext. There are four major steps involved in this algorithm. They are: Key Expansion, Initial Round, Rounds and Final Round.

In the first stage they round keys are derived from the cipher key using key schedule. AES requires a separate 128-bit round key block for each round plus one more. In the second stage AddRoundKey is used in each byte of the state is combined with a block of the round key using bitwise xor. In the third stage, SubBytes is a non-linear substitution step where each byte is replaced with another according to a lookup table. ShiftRows is a transportation step where the last three rows of the state are shifted cyclically a certain number of steps. MixColumns is a mixing operation which operates on the columns of the state, combining the four bytes in each column. AddRoundKey in which the sub key is combined with the state. The sub key is added by combining each byte of the state with the corresponding byte of thesub key using bitwise XOR.

A. NFC-SEC: NFCIP-1 Security Services and Protocol

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. The major mechanism provided by NFCIP-1 is SDD (Single Device Detection) and RFCA (Radio Field Collision Avoidance).

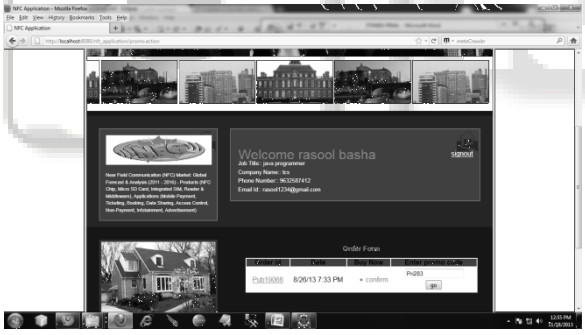

Fig. 3: Entering the Private Key for getting the bill details

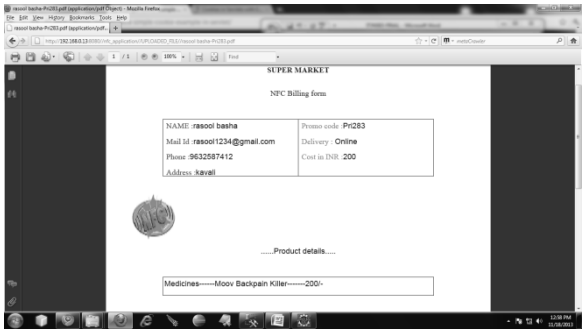

Fig. 4: Security Key is generated by the bank

The SDD is an algorithm for initiator to find a specific target among multiple targets in the RF field. In existing RFID system, collision problem may occur. The collision is referred to as a state in which more than two initiators or targets transmit data at the same time, and it is impossible to distinguish which data is real. The collision problem is solved by NFC standard using algorithm named RFCA. RFCA is an algorithm that detects other RF fields and prevents collision using carrier frequency. RFCA begins by confirming the presence of other RF fields. If other RF fields exist, the NFC does not generate its own RF field. Thanks to the SDD that finds specific target within the range and RFCA that does not permit 2 RF fields, the NFC can be safe from MITM (Man-In-The-Middle) attacks.

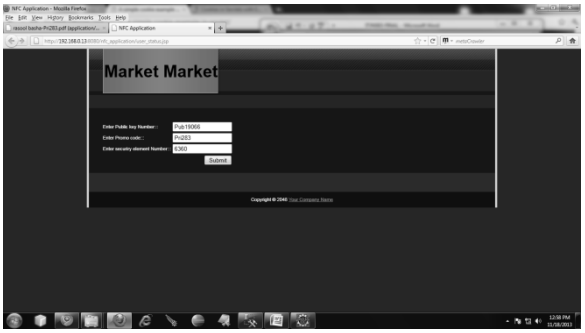

Fig. 5: Three Keys namely Public Key, Private Key and Security Key are entered

VI. PSEUDONYM

Pseudonym represents ID that changes randomly, it has been widely used in order to remove the linkages between the messages.The pseudonyms are composed of public key, private key, and a certificate. Users can be assured of their anonymity through pseudonym and authenticated as normal users through a certificate. The TTP stores pseudonyms and actual ID of users to reveal the anonymity in case of a problem. However, the method using the pseudonym requires additional costs for storage and communication.

VII. CONCLUSION

The data used to help a future purchase uses protected PDU of NFC-SEC, and data not wanted to be recorded uses conditional privacy PDU selectively, which makes it possible to remove the connectivity with the existing messages.With recent release of various terminals equipped with NFC (Near Field Communication), e-payment market using NFC is expected to be activated. In such situation, the user's transaction information leaks can lead to the invasion of privacy. In this paper, the conditional privacy protection methods are proposed to solve the aforementioned problems. The proposed method uses random public key like pseudonyms. Since the public key is updated, fewer burdens are imposed on the administration.

REFERENCES

[1] "Announcing the ADVANCED ENCRYPTION STANDARD (AES)". Federal Information Processing Standards Publication 197. United States National Institute of Standards and Technology (NIST). November 26, 2001.
[2] Daemon, Joan: Rijmen, Vincent "AES Proposal: Rijndael". National Institute of Science and Technology. February 21, 2013.
[3] John Schwartz "U.S. Selects a New Encryption Technique". New York Times, October 3, 2000.

[4] Westlund, Harold B "NIST reports measurable success of Advanced Encryption Standard". Journal of Research of the National Institute of Science and Technology, 2002.
[5] Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson, Tadayoshi Kohno, Mike Stay "The Two fish Team's Final Comments on AES Selection", May 2000.
[6] ISO/IEC 13157-1:2010, "Information technology Telecommunications and information exchange between systems – NFC Security – Part 1: NFC-SEC NFCIP-1 security service and protocol," ISO/IEC, May 2010.
[7] ISO/IEC 13157-2:2010, "Information technology Telecommunications and information exchange between systems – NFC Security – Part 2: NFC-SEC cryptography standard using ECDH and AES," ISO/IEC, May2010.
[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] A. Chandrasekar, V.R. Rajasekar, and V. Vaasudevan, "Improved authentication and key agreement protocol using elliptic curve cryptography," International Journal of Computer Science and Security (IJCSS), Vol. 3, Issue 4, pp. 325-333, Oct. 2009.
[10] Juniper Research, "NFC Mobile Payments & Retail Marketing – Business Models & Forecasts 2012-2017," May 2012.
[11] J. Yu, W. Lee, and D.-Z. Du, "Reducing Reader Collision for Mobile RFID," IEEE Transactions on Consumer Electronics, Vol. 57, No. 2, pp. 574-582, May 2011.

