An Empirical Survey on Various Malicious Security Attacks in Online Transactions

B.T.Geetha[1], M.V.Srinath[2], Mr.V.Perumal[3]

[1]Research Scholar,Sathyabama University, Chennai, India
[2]Head – Content Development, Efuture Soft, Chennai, India,
[3]Associate professor, Saveetha Engineering College, Chennai, India

Abstract— *Even with several technological developments and security protocols, the electronic payment is still not in safe waters. Today we come across several frauds related to this electronic payment, the main reason for this is that user data like passwords, account numbers and other private information of the user is accessed by unauthorized persons. The permanent solution to this to protect the user privacy, to secure the users confidential information from the grasps of the hackers by developing a foul proof protocol. Therefore a new security protocol has to be laid, where user identity is hidden and the public key of the user is secured from the attacks of the hacker. Conditional privacy method using pseudonyms is used to avoid several threatening attacks such as MITM attack (Man-In-The-Middle attack), Eavesdropping and Data modulation in e-payment.*

Keywords--- Conditional privacy, MITM-Man in the Middle, Data Modulation, Eavesdropping.

I. INTRODUCTION

Online shopping, online money transfers and online banking save us a lot of time and make our lives easier. However, these same technologies also make life easier for cybercriminals by offering them new and easy ways to steal users' money. Using stolen payment data is an effective and popular way of making a quick profit. Although banks try to protect their customers, attacks against individual users are still quite common.

Hacking a bank is more time-consuming and expensive and the risk of being caught is higher. By contrast, many individual customers use computers with numerous vulnerabilities, which are easier to compromise. By stealing a relatively small amount from each hijacked online banking account, a cybercriminal has a good chance of going undetected. Significantly, attacks against individual customers are largely automated and require almost no operator involvement.

The key agreement done during the establishment of connection between the sender and the receiver plays an important role in secured transactions. It is important that the public key of the users are hidden or else it is possible that hackers using this public can manipulate the user data and illegally access their accounts. The public key and the private key of the user are needed to be encrypted by the use of security protocols were the privacy is protected and user data is secure.

II. LITERATURE SURVEY

2.1 Survey Paper-1

2.1.1. Introduction

In This paper Thomas Plos et..al represents the design and implementation of a complete near-field communication (NFC)[1] tag system that supports high-security features. The tag design contains all hardware modules required for a practical realization, which are: an analog 13.56-MHz radio-frequency identification (RFID) front-end, a digital part that includes a tiny (programmable) 8-b microcontroller, a framing logic for data transmission, a memory unit, and a crypto unit.

2.1.2 Technology Used

In this paper the security features includes support of encryption and decryption using the **Advanced Encryption Standard (AES-128)**, the generation of digital signatures using **the elliptic curve digital signature algorithm** according to NIST P-192, and several countermeasures against common implementation attacks, such as side-channel attacks and fault analyses. The chip has been fabricated in a 0.35-µm CMOS process technology, and requires 49 999 GEs of chip area in total (including digital parts and analog front-end). Finally, we present a practical realization of our design that can be powered passively by a conventional NFC-enabled mobile phone for realizing proof-of-origin applications to prevent counterfeiting of goods, or to provide location-aware services using **RFID** technology.

2.1.3 Advantages

The flexible tag architecture allows secure communication between the devices using Near Field Communication as this system uses asymmetric key process the authentication process is secure and it consumes less power.

2.1.4 Drawbacks

The system is having a quite complex design and it requires 49 999 GEs of chip area which makes it hard to design.

2.1.5 Results

The tag is implemented in a 0.35-µm CMOS technology using a semi-custom design flow with Cadence RTL Compiler as synthesis tool. In total, the chip needs 49 999 GEs, microcontroller needs around 19%, including instruction unit, ALU, PC, register file (about 65 GEs per register), and program ROM. The data path and the pattern sequencer of the CU take about 15% of the chip area, i.e., 7488 GEs (this number does not include the ROM for ECDSA, AES, and SHA-1 program and the needed constants).

TABLE I

AREA OF CHIP COMPONENTS

Component	GEs	%
Analog front-end	8100	16.20
FL	2663	5.33
8-b microcontroller		
Instruction decode unit, ALU, and PC	945	1.89
Register file (26 × 8-b)	1693	3.38
Program ROM (2027 × 16-b)	6764	13.53
Bus arbiter	319	0.64
CU		
Micro-code pattern sequencer	3880	7.76
Datapath (ECDSA, AES, and SHA-1)	3608	7.22
Memory unit		
EEPROM (256 × 16-b)	12 700	25.40
ROM (CU constants)	600	1.20
RAM macro (128 × 16-b)	8727	17.45
Total	**49 999**	**100.00**

2.2. Survey Paper-2

2.2.1 Introduction

In this paper, a short message service (SMS) based m-banking protocol under GSM technology is presented. In view of ensuring a high level of security during client authentication and data transmission, in the proposed SMS-banking scheme, a digital watermarking technique is introduced

2.2.2 Technology

The method proposed here uses text watermarking for hiding the SMS containing transaction information into another dummy text file (DTF) in order to make the transactions unnoticeable to the intruder. **Digital watermarking methods** for text are rather limited because of the binary nature of text documents which lack rich gray scale information. The basic requirements to be fulfilled for digital watermarking are imperceptibly, security, and robustness. In this paper, we introduce a new idea where a special emphasis is given on the robustness and security of the information hidden rather than of the **DTF**.

So unlike conventional watermarking, the DTF is changed more or less depending on the embedded information. This however does not result any loss of information as the DTF can be easily retrieved in accordance with the access code, which was sent from the BS in the first case. The DTF simply acts as an imperceptible carrier of the SMS containing transaction information. As specified by **GSM** 03.38, an SMS contains 7 bit default alphabet comprising of alphanumeric and other special characters .

2.2.3 Advantages

SMS Banking is made secure by using Digital Watermarking Method, privacy and the identity of the users are protected from unauthorized persons.

2.2.4 Drawbacks

GSM based system are prone to security attacks, since the algorithm used provide security only to the user data and not to the network and also problem may arise if there is no signal from the tower or due to tower failure signals are lost and also during handoff, hand over process collisions are said to occur in the network.

2.2.5 Results

The proposed scheme guarantees a high level of security because of the introduction of digital watermarking for client authentication and data transmission. The Accuracy vs Numbers layers flipped graph is given by:

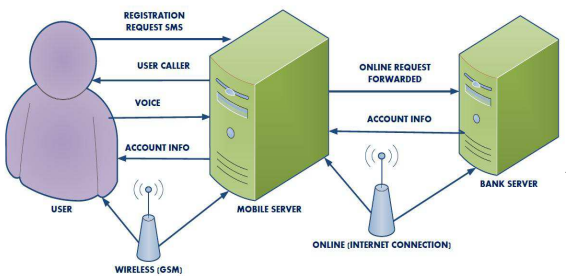

Fig.1 Service Request

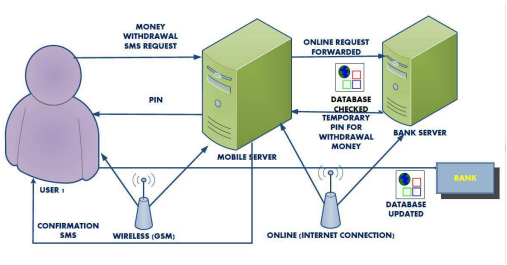

Fig.2 Transaction Procedure

2.3. Survey Paper-3

2.31 .Introduction

In this paper, we are preserving database from malicious attacks. We are storing encrypted data in database which can be easily hacked. By using attribute based encryption technique we could preserve the confidentiality of database even if server is untrusted, also we are preventing the collusion attacks using collusion avoider protocol.

2.3.2. Technology

In this proposed paper we use attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt .our methods are same as Role based access control (RBAC). In this paper we provide **cipher text-policy attribute based encryption(ABE).** It is an alternative for public key encryption. By our proposed method **collusion resistant .**It is assured by using shared scheme and embedding independently chosen secret shares into each private key. We use novel private key randomization technique that uses two level random masking methodology. This method makes uses of group with efficiently computable bilinear group model.

2.3.**3 Advantages**

Encrypted data can be safely stored in a database using attribute based encryption techniques and collusion can be avoided. This method preserves the user private data such as passwords, username, bank account number etc.. from unauthorized persons.

2.3.4 Drawbacks

Encryption and decryption of cypher text takes longer time than usual method also cypher text. data is around 160 bit which requires more memory for storage

2.3.5 Results

The proposed scheme provides high level of secure data transmission when data are stored in prone database and also it avoids collision so that hacker cannot decrypt the cypher text.

2.4. Survey Paper-4

2.4.1 Introduction

In this paper, we are preserving the spoofing of the password from dictionary attacks using augmented encryption key exchange protocol by using this protocol attacker obtains insufficient information to mount dictionary attacks. In this method password are stored using hash table which provide high level of security. Security against dictionary attacks using augmented encryption key exchange protocol is the best method for securing user data,

2.4.2 Technology

In this paper we propose a **Encryption key exchange protocol (EKE)** which is augmented so that host that the host do not store the clear text password**.** We use (EKE) to avoid dictionary attacks,(EKE) can be easily implemented by using **Digital signature** which relies on the one way commutative one way functions.(EKE) provides authentication and long term storage of a simple password. In this paper we use Encryption key exchange protocol (EKE) along with **Hashing function** to hash the password which is mainly done to avoid dictionary attack and collusion attacks of the password. Digital signature can also be used with EKE to encrypt the password which offers more efficiency than the hashing function for the Digital signature of the password we use **RSA algorithm** along with **Elliptic curve** for the generation of the pseudo random number.

2.4.3 Advantages

This method offers more security to the password f2rom an attacker who is unaware of hash function and from an attacker who know about the hash function can neither be able to mimic the host nor able to get useful information about password.

2.4.4 Disadvantages

This method does not protects the data against the intruder who has captured the host copy of the authentication data. Augmented encryption key exchange is based on public key exchange so it a drawback.

TABLE-2 COMPARISON OF MOBILE WIRELESS NETWORKS

Mobile wireless	User mobilit	Coverage	Terminals	Applications

network	y level	Area		
GSM	high	Outdoor (order of kilometres)	cell phone	Voice calls
802.11	low	Indoor (< 100m)	laptop, PDA	Internet, e-commerce
Bluetooth	low	Indoor (< 10 meters)	peripheral devices	Replacement of wires connecting devices in close proximity of each other

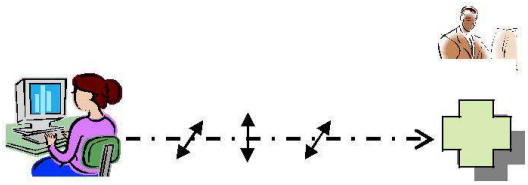

Fig.3 Transaction Procedure

2.4.5 Results

The proposed paper suggest high level of security to the password using encryption key exchange using digital signatures and also by using public key encryption key exchange. These methods prevents password from dictionary attacks also spoofing can be avoided.

2.5 Survey Paper-5

2.5.1 Introduction

In this paper we propose quantum cryptography techniques to provide promising level of security to the existing cryptography techniques. Quantum cryptography can be applied to mobile wireless networks, it easily detect the eaves dropping .It generates the secret key for each time

2.5.2 Technology

In this paper we device a quantum cryptography technique which overcome the drawbacks in the existing cryptography techniques. Quantum cryptography which relies on the quantum key distribution when applied to fibre optic network will offer a better performance then existing method. quantum key distribution technique is equipped in mobile wireless networks especially we use Global system for mobile communication (GSM) it will solve the line of sight problem between the satellite and ground station. Quantum cryptography offers the EAP-based authentication between the supplicant and the authentication server, the PMK is derived by the mobile device and the authentication server from the AAA (Authentication, Authorization and Accounting) key. The EAP-based authentication and PMK establishment between the supplicant and the authentication server. The Pairwise Transient Key (PTK) is established between the access point and the mobile terminal during the 4-way handshake.

2.5.3 .Advantages

Quantum key cryptography is offering high degree of security to wireless sensor network than the existing cryptography techniques.

2.5.4 Drawbacks

GSM based system are prone to security attacks, since the algorithm used provide security only to the user data and not to the network.

2.5.5 Results

In this paper we are suggesting quantum cryptography based technique for the wireless mobile. Quantum cryptography can be used in 802.11i supporting standard for the variety of the applications network it provides high level of security than the existing cryptography techniques.

III. PROPOSED SYSTEM

In this paper, 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.

NOTATION

otation	Description
1)	Concatenation symbol
N_X	Nonce of user X
ID_X	Random ID of user X for the activation of transport protocols
QX, QX', QX''	Compressed elliptic curve public key of user X
Q_X, Q'_X, Q''_X	Elliptic curve public key of user X
d_X	Elliptic curve private key of user X
G	Elliptic curve base point
KDF	Key derivation function
$MacTag_X$	Key verification tag received from X

MK	Shared secret key
z	Unsigned integer
r_X	Random integer generated by user *X*
PN	Pseudonym set
Enc(*k*, *m*)	Encrypt *m* with *k*
Sig(*k*, *m*)	Signature on *m* with *k*

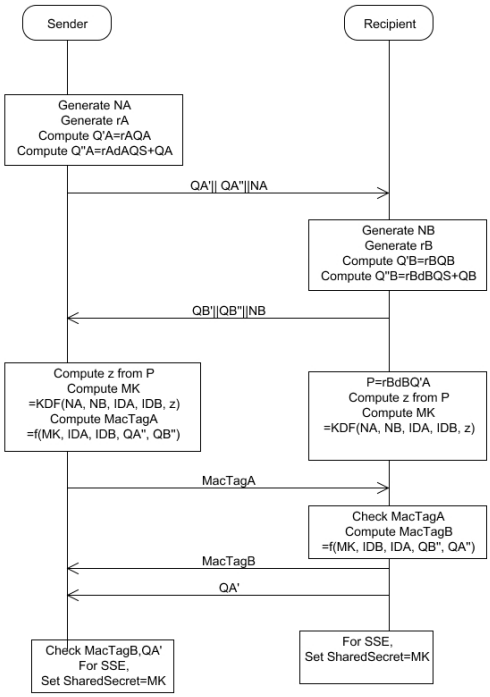

Fig. 4. Block Diagram

IV. CONCLUSION

The proposed methods follows standard systems, additionally can hide user's identity, and if necessary, the user's identity can be confirmed by the TSM. Also the user can get personalized services by the selective use of our proposed method.

In conclusion, it is expected that the proposed method will help users to protect their privacy and use personalized services. It will contribute to the promotion of mobile payment services through NFC.

REFERENCES

[1] Security-Enabled Near-Field Communication Tag With Flexible Architecture Supporting Asymmetric Cryptography by Thomas Plos, Michael Hutter, Martin Feldhofer, Maksimiljan Stiglic, and Francesco Cavaliere.

[2] Security Enhancement Protocol in SMS-Banking using Digital Watermarking Technique by Md. Nazmus Sakib, A B M Rafi Sazzad, Syed Bahauddin Alam,Celia Shahnaz , Shaikh Anowarul Fattah Bangladesh University of Engineering and Technology,

[3] Ciphertext-policy attribute-based encryption techniques IEEE conference 2009.

[4] Security against dictionary attacks using augmented encryption key exchange protocol IEEE Lournal and Magazines on security.

[5] Security of mobile wireless networks based on 802.11i Encryption key distribution using quantum cryptography

[6] Gartner, "Market Insight: The Outlook on Mobile Payment," Market Analysis and Statistics, May 2010.

[7] Juniper Research, "NFC Mobile Payments & Retail Marketing – Business Models & Forecasts 2012-2017," May 2012.

[8] ISO/IEC 15946-1:2008, "Information technology – Security methods – ryptographic methods based on elliptic curves – Part 1: General," Apr. 2008.

[9] 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.

[10] ISO/IEC131572:2010,"InformationtechnologyTelecommunicationsand information exchange between systems – NFC Security – Part 2: NFC-SEC cryptography standard using ECDH and AES," ISO/IEC, May 2010.

[11] H. Eun, H. Lee, J. Son, S. Kim, and H. Oh, "Conditional privacy preserving security protocol for NFC applications," IEEE International Conference on Consumer Electronics (ICCE), pp. 380-381, Jan. 2012.

[12] ISO/IEC18092:2004,"Informationtechnology – Telecommunications and information exchange between systems – Near field Communication – Interface and Protocol (NFCIP-1)," ISO/IEC, Apr. 2004.

[13] 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.

[14] E. Haselsteiner and K. Breitfuß, "Security in Near field Communication (NFC) – Strengths and Weaknesses –," RFIDSec 2006, Jul. 2006.

[15] IEEE Std. 1363-2000, IEEE Standard Specifications for Public-Key Cryptography, Jan. 2000.

[16] G. Calandriello, P. Papadimitratos, J.P. Hubaux, and A. Lioy, Efficient and robust pseudonymous authentication in VANET," Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks (VANET 2007), pp. 19-28, 2007.

[17] J.C.M. Teo, L.H. Ngoh, and H. Guo, "An Anonymous DoS-Resistant Password-Based Authentication, Key Exchange and Pseudonym Delivery Protocol for Vehicular Networks," Proceedings of the 2009 International Conference on Advanced Information Networking and Applications (AINA 2009), pp. 675-682, May 2009.

[18] D. Eckhoff, C. Sommer, T. Gansen, R. German, and F. Dressler, "Strong and affordable location 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.

[19] J.-H. Lee, J. Chen, and T. Ernst, "Securing mobile network prefix provisioning for NEMO based vehicular networks," Mathematical and Computer Modelling, vol. 55, No. 1, pp. 170-187, Jan. 2012.