International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 1 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT195199

Secure Micro Payment Using Physical Unclonable Function

[1]M. Jalasri, [2]S. Nalini, [3]N. Magesh Kumar, [4]J. Elumalai
[1,2,3,4]Assistant Professor, Information Technology, Jeppiaar Maamallan Engineering College, Sriperumbudur, Tamil Nadu, India

ABSTRACT

In online aggressors regularly go for taking such client information. In these situations, malware that can take card information when they are perused by the gadget has thrived. This framework gives secure micro-payment and enhances date approaches in terms of security. In proposed system, utilize two principle capacities PUF (Physical Unclonable Function) and FRoDo(Fraud Resilient Device for Off-Line Micro-Payments). These two can be given security to installment process and client account. These produce double encryption to protect the system from attackers. In proposed system gives more security for transaction.

Keywords : Mobile Secure Payment, Architecture, Protocols, Advance Encryption, Fraud-Resilience

I. INTRODUCTION

Mobile commerce is one of the future research areas, especially for mobile payment systems. In the existing system, the payments are performed on the fixed cellular network which degrades security. To enhance security on transaction and payment process by performing e-payment systems in the distributed development of the wireless ad-hoc network [1].

In Modern cryptographic, only authorized parties can acquire secret keys and access information. Be that as it may, different sorts of altering techniques have been concocted to separate secrecy keys from restrictive access frameworks, for example, smartcards and ATMs. This server authenticates the PUF by two kinds of error probabilities such as false alarm rate (FAR) and false detection rate (FDR) [2].

The main goal of this paper is to introduce the variety of devices for influence magnetic stripe card data and demonstrate magnetic stripe cards by fraudulently cloned and analyze how such devices can be processed. This technique used for personal identification and authentication but very difficult to exchange key to card issuers [3].

FRoDO highlights a character component to confirm the client, and a coin component where coins are not privately put away, but rather are registered on-the fly when required.

Payment transaction does not directly read customer coins. The vendor only communicates with the identity element in order to identify the user.The main benefit is a simpler, faster, and more secure interaction between the involved actors/entities. The identity element used to improve the security of the users. This provide more secure off-line payments.

.

II. RELATED WORK

A TPM (Trusted Platform Module) is a standard for securing hardware device with the help of incorporated cryptographic keys. Here identify attacks only in memory and bus probing not real word attacks [4].

Near Field Communication (NFC) technology is a short-range wireless communication between the devices. NFC used in credit card, e-ticket, and mobile payment. It provides security for m-payment systems and also eases of use for the user. The main issue in this system is unable to receive phone calls when processing payment operation [5].

Symmetric key cryptography which reduces computation at all the entities of the protocol. Kungpisdan et al and Tellez said this security protocol satisfies the existing standard protocols like SET. But lack of complexity produced during transaction and identification of users [6]. However, the solutions are limited in that protocols require at least one of the two parties to be online, i.e. connected either to a trusted third party or to a shared database.

FORCE (Fully off-line secure credits for mobile micro payments) exclusively perform the operations at catching the topological impact introduced by the wormhole. Detection of wormholes is successfully done without any overhead or need of external devices to monitor the network. But, difficult to share database to trusted third party it didn't notice any real time attacks such as skimmers, scrapers and data vulnerabilities [7].

III. IMPLEMENTATION WORK

Architecture Diagram for secure micro payment using physical unclonable function in Figure 1. User is registered first before login. Vendor is registered first before login. Vendor Details are Stored in Database. Vendor is waiting for activation. Vendors get transaction after activation. Frodo view the user who gives request to activation and Frodo activate the user. After activation user login into account to gives payment request. After PUF verification Payment transaction will success.

A. CLIENT MODULE:

Fig. 2. Client module. User is registered first before login. User and Vendor are waiting for activation. Customer gives the payment request after Activation. Users are activated by Frodo. Gives bank name, permanent card number and its pin number to registration. User Details are Stored in Database.

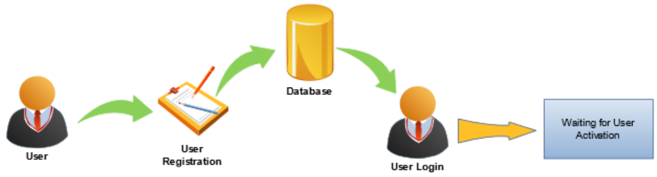

Fig. 2. Client module

B. VENDOR MODULE:

In fig. 3 Vendor is registered first before login. Vendor Details are Stored in Database. Vendor is waiting for activation. Vendors get transaction after activation. Users and Vendors are activated by Frodo. Gives bank name, Branch and password to registration.

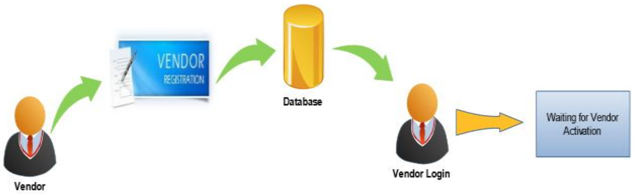

Fig. 2. Vendor module

C. KEY GENERATION

Frodo view the user who gives request to activation and Frodo activate the user. Identity element is generating private key to the user and coin element generate binary code for user account number into binary code. This two-step makes Payment more secure. Key Generator used generate the private key of the identity element and symmetric and asymmetric cryptographic algorithms applied to data received in input and sent as output by the identity element in fig, 3.

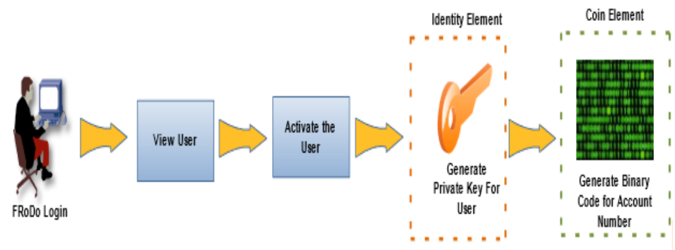
Identity Element
Coin Element
FRoDo Login
View User
Activate the User
Generate Private Key For User
Generate Binary Code for Account Number

Fig. 3. Key Generation

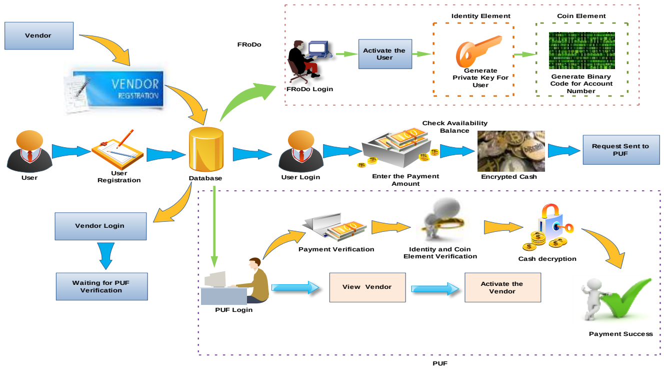

Fig. 4. Architecture Diagram for secure micro payment using physical unclonable function.

The Rivest-Shamir-Adleman(RSA) public key cryptography algorithm which is used to encrypt a message. The RSA algorithm performs public key encryption and digital signatures.

1. Represent the message as a whole number in the vicinity of 0 and (n-1). Huge messages can be separated into various squares. Each piece would then be spoken to by a whole number in a similar range.

2. Encrypt the message by raising it to the eth control modulo n. The outcome is a ciphertext message C.

3. To unscramble ciphertext message C, raise it to another power d modulo n

The encryption key (e,n) is made open. The unscrambling key (d,n) is kept private by the client.

D. PAYMENT REQUEST

After activation user login into account to gives payment request in fig. 4. Enter the required payment and Check the availability of payment for customer requirement. Required amount encrypted using key and after payment request goes to PUF verification. After PUF verification Payment transaction will success.

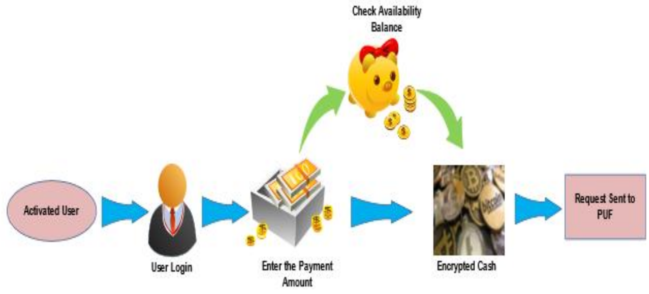

Fig. 4. Payment request

In cryptography, (Advance Encryption Standard)AES is broadly embraced and upheld in both equipment and programming. Cryptanalytic attacks against AES has not been discovered practically. A degree of 'future-proofing' allowed by AES which has flexibility of key length.

In any case, similarly with respect to DES, the AES security is guaranteed just in the event that it is effectively actualized and great key administration is utilized.

E. PUF PROCESS:

Heart of FRoDO proposal lies a read-once strong physical unclonable function. In fig.5 PUF check vendors details involved in payment and activate the vendors.

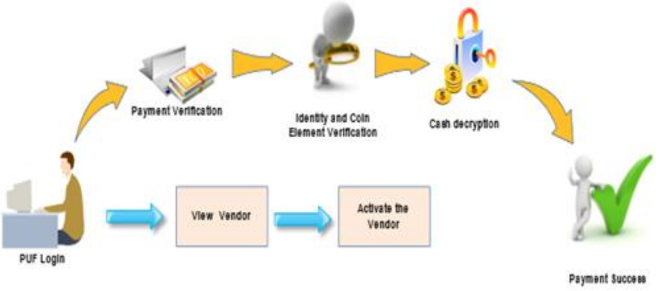

Fig. 5. Puf process

In payment verification PUF check both Identity and Coin Element. After verification payment decrypted using public key and the payment transaction completed successfully and whole transaction will be secure. Finally receives the Private Response, the last step only requires the coin just read to be validated. Then, the whole payment transaction can be authorized and committed.

IV. CONCLUSION

Security analysis shows proposed system does not impose trustworthiness assumptions.Further, it is also the first solution in the literature where no customer device data attacks can be exploited to compromise the system This has been accomplished basically by utilizing a novel erasable PUF engineering and a novel convention outline. Furthermore, our proposal has been thoroughly discussed and compared against the state of the art. Our investigation demonstrates that it is the main suggestion that appreciates every one of the properties required to a safe small scale installment arrangement, while likewise presenting adaptability while thinking about the installment medium (kinds of advanced coins).

Finally, some open issues have been identified that are left as future work. Specifically, examining the likelihood to enable computerized change to be spent over various disconnected exchanges while keeping up a similar level of security and ease of use. In FRoDO, develop to access money without standard coin element. In future, try to enhance the capability of the AES algorithm to a generate private key and create more security for Electronic payments. Another approach will involve smarter implementation of secure offline transfer of money by using PUF.

V. REFERENCES

[1]. N. Chitra Kiran, G. Narendra Kumar, “Building robust m-commerce payment system on offline wireless network”,2011 Fifth IEEE International Conference on Advanced Telecommunication Systems and Networks (ANTS) , March 2012

[2]. D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, “Extracting secret keys from integrated circuits,” IEEE Trans. Very Large Scale Integr. Syst., vol. 13, no. 10, pp. 1200–1205, Oct. 2005.

[3]. G. Hong and J. Bo, “Forensic analysis of skimming devices for credit fraud detection”, 2nd IEEE Int. Conf. Inf. Financial Eng., Sep. 2010

[4]. P. Choi and D. K. Kim, “Design of security enhanced TPM chipagainst invasive physical attacks”,IEEE Int. Symp. Circuits Syst., pp. 1787–1790,2012.

[5]. W. Chen, G. Hancke, K. Mayes, Y. Lien, and J.-H. Chiu, “Using 3G network components to enable NFC mobile transactions and authentication”, IEEE Int. Conf. Progress Informat. Comput., Dec. 2010, vol. 1, pp. 441–448.

[6]. V. C. Sekhar and S. Mrudula, “A complete secure customer centric anonymous payment in a digital ecosystem”, Int. Conf. Comput., Electron. Elect. Technol., 2012, pp. 1049–1054.

[7]. V. Daza, R. Di Pietro, F. Lombardi, and M. Signorini, “FORCE: Fully off-line secure credits for mobile micro payments”, 11th Int. Conf. Security Cryptography, 2014, pp. 125–136.

[8]. S. Golovashych, “The technology of identification and authentication of financial transactions. from smart cards to NFC-terminals”, IEEE Intell. Data Acquisition Adv. Comput. Syst., Sep. 2005, pp. 407–412.

[9]. Slava Gomzin, “Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions, Computing & Technology 1st ed. New York, NY, USA: Wiley, 2014.

[10]. Meng-Day Yu, Srinivas Devadas “Secure and robust error correction for physical unclonablefunctions”, IEEE Design & Test of Computers , vol. 27, no. 1, pp. 48–65, Jan. 2010.

Cite this article as : M. Jalasri, S. Nalini, N. Magesh Kumar, J. Elumalai, "Secure Micro Payment Using Physical Unclonable Function", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 1, pp. 483-486, January-February 2019. Available at doi : https://doi.org/10.32628/CSEIT195199
Journal URL : http://ijsrcseit.com/CSEIT195199