Sixth International Conference on Emerging trends in Engineering and Technology (ICETET'16)
www.ijera.com
ISSN: 2248-9622, pp.55-58

RESEARCH ARTICLE OPEN ACCESS

Secure Payment Solutions Fully Off-Line Functions on Frodo

[1]S.Balaji, [2] G. Amutha, [3] R. Subha,
[1] Assistant Professor, [2] Pg Scholar, [3] Pg Scholar
Department Of Computer Science, SCAD College Of Engineering and Technology, Tirunelveli, Tamil Nadu

ABSTRACT:
Online shopping payment scheme is one of the popular in recent years. During payment process the attackers aim to stealing the customer data by targeting the Point of Sale (PoS) system. Increasing malware that can steal card data as soon as they are read by the device. As such, in cases where customer and vendor are steadily or intermittently disconnected from the network and there is no secure during on-line payment. We proposed work is to provide secure fully off-line work is interactivity between multiple client - server.This server is identified from legal to illegal control is provided to customer key approach. Once collect the details at customer side are customer account is disable automatically by erasable PUFs . It include that limited activity is ensured referred as server to client transaction is secured. Further, an exhaustive investigation of FRODO utilitarian and security properties is given, demonstrating its viability and plausibility.
Keywords: Secure payments, PoS system, erasable PUFs ,fraud resilience, cybercrime.

I. INTRODUCTION

Nowadays online payments are one of the most popular, when the customer or buyer makes his payment transactions for the goods purchased with the use of the online money payment. In that the purchase methods from classic credit or debit cards to new approaches like mobile-based payments, giving new market entrants novel business probabilities. However, many of us still resist the attractiveness and ease of revolving credit transactions because of security issues. so far there are a high risk for taken cards, fraud so the purchasers worry debit-card fraud by merchants and different third parties. Payment transactions are usually processed by an electronic payment system (for short, EPS). The EPS is a separate function from the typical point of sale function, although the EPS and PoS system may be co-located on constant machine. In general, the EPS performs all payment process, whereas the PoS system is that the tool utilized by the cashier or shopper. Point of Sale is the time and place where a retail exchange is finished . At the point of sale, the dealer would set up a receipt for the client or generally figure the sum owed by the client and give choices to the client to make payment. In these transaction process, there is chance to attackers often aim at stealing such customer data by targeting the Point of Sale. Modern PoS systems are powerful computers equipped with a card reader and running specialized software. Increasingly typically, user devices are utilized as input to the PoS. In these scenarios, malware that can take card information when they are read by the device has thrived. So that we proposed FRODO techniques, a safe disconnected from the net transaction arrangement that is strong to PoS information breaches. Our solution enhances over exceptional methodologies as far as adaptability and security.

II. RELATED WORK

Mobile payment solutions proposed so far can classified as totally on-line [2] semi off-line [6], weak off-line or totally off-line [10]. The most issue with a totally off-line approach is that the problem of checking the trait of a dealings while not a trusty third party. In fact, keeping track of past transactions with no out there association to external parties or shared databases is quite tough, because it is tough for a trafficker to ascertain if some digital coins have already been spent. This is often the most reason why throughout previous couple of years, many alternative approaches are planned to produce a reliable offline payment theme. Though several works are revealed, all of them targeted on dealings namelessness and coin unforgeability.

III. PROBLEM STATEMENT

Attackers usually aim at stealing such customer data by targeting the point of Sale (for short, PoS) system, i.e. the point at that a marketer initial acquires customer data. Fashionable PoS frameworks are effective computers furnished with a card reader and running particular software package. In these eventualities, increasing malware that steal card information as presently as they are scan by the device. As such, in cases wherever customer and vendor are steady or intermittently disconnected from the network,and no secure throughout on-line payment.

IV. PROPOSED SYSTEM

The proposed system which modules are discuss the payment system and set of processes of technologies that transfer price from one entity or person to a different. Payments area unit usually created in exchange for the availability of products, services, or to satisfy a legal obligation. They will be created during a type of currencies victimization many strategies like money, checks, electronic payments and cards. The essence of a payment system is that it uses cash-substitutes, like checks or electronic messages, to make the debits and credits that transfer worth.

Proposed Architecture

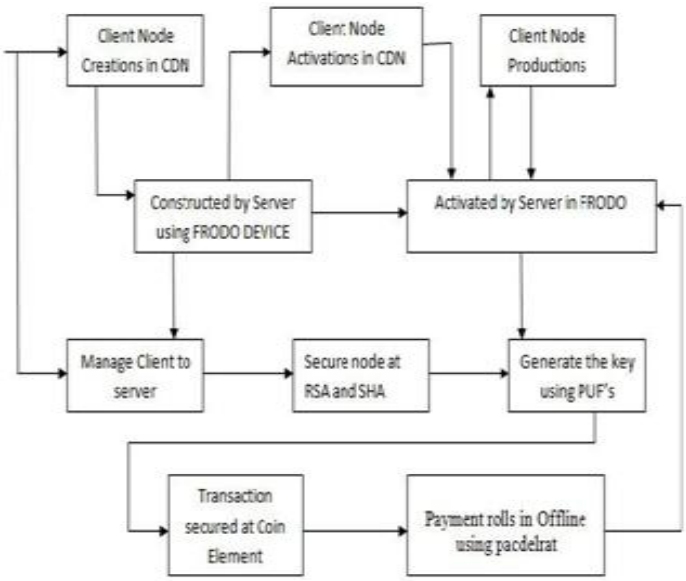

Fig1. System Architecture

V. EXPERIMENTS

Client Module

This module used to client are going to online website. And View Product and select to product models and view product details. Select and purchase their product .and transaction from their account All details are encrypted by using Private Key and public key, Keys are generated during user to purchase the product.

Key Generator:

This module is using cryptographic algorithm, this algorithm used for symmetric and asymmetric cryptographic algorithms applied to received the data input and sent as output by the identity element. Key Generator is by PUFs, which have been used to implement strong challenge-response authentication. Also,multiple physical unclonable functions are used to authenticate both the identity element and the coin element.

Secure payment:

This module is used to Users are view products, and select products and their details and to be wish to purchase product and give all sensitive data like account details, payment details. All user information is encrypted because hackers do not hacking user information. All Encrypted data are separated by symmetric and Asymmetric cryptographic algorithms this is used to separate private and public keys. Private Key is send to user mail. User is used this key to view their purchase product and transaction their account.

Transaction at Coin Element:

This module is used to admin to work their website and add products like product name, description, warrenty period,etc., and admin view all users purchase products but cannot view user account details. and to view which product is delivered or not.

VI. PERFORMANCE ANALYSIS

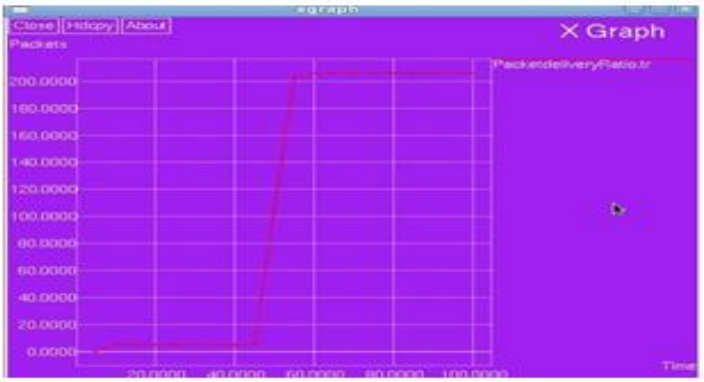

Fig2. Packet Delivery Ratio

The Performance Analysis is generated to check wheather the data is transmitted between the Client and Server in a error free manner. It can avoid the data loss during the transmission. So the client can make use of data in a efficient manner.

VII. SECURITY ANALYSIS

Authenticity

It is guaranteed in FRODO by the on-the-fly computation of private keys. In fact, both the identity and the coin element use the key generator to compute their private key needed to encrypt and decrypt all the messages exchanged in the protocol. Furthermore, each public key used by both the vendor and the identity/coin element is signed by the bank. As such, its authenticity can always be verified by the vendor.

Availability

The availability of the proposed solution is guaranteed mainly by the fully off-line scenario that completely removes any type of external communication requirement and makes it possible to use off-line digital coins also in extreme situations with no network coverage. Furthermore, the lack of any registration or withdrawal phase, makes FRoDO able to be used by different devices.

Confidentiality

Both the communications between the customer and the vendor and those between the identity element and the coin element leverage asymmetric encryption primitives to achieve message confidentiality.

Non-Repudiation

The storage device that is kept physically safe by the vendor prevents the adversary from being able to delete past transactions, thus protecting against malicious repudiation requests. Furthermore, the content of the storage device can be backed up and exported to a secondary equipment, such as pen drives, in order to make it even harder for an adversary to tamper with the transaction history.

VIII. RESULTS & DISCUSSIONS

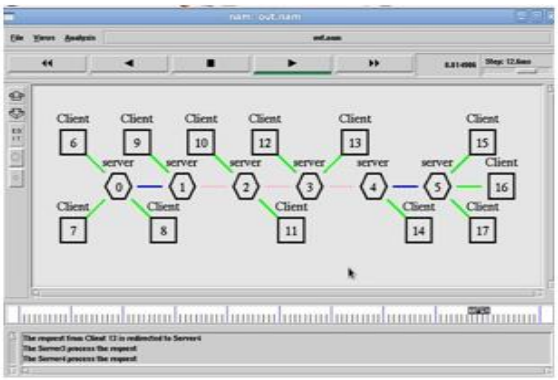

Fig3. Key Generator

Initially, the Client send the transmission request to the Server. Then the Server starts up. The Server contains all the data that the Client needs. In order to secure the transmission of data, the client generates the key during the transmission. It is used for Encryption and decryption purpose. After the key is generated between the Client and the Server, the data transmission occurs. Once the key is accepted, the data

IX. CONCLUSION AND FUTURE WORK

We have introduced FRODO that is, to the best of our knowledge, the first data-breach-resilient fully off-line micropayment approach. The security analysis shows that FRODO does not impose trustworthiness assumptions. Further, FRODO is also the first solution in the literature where no customer device data attacks can be exploited to compromise the system. This has been achieved mainly by leveraging a novel erasable PUF architecture and a novel protocol design. Furthermore, our proposal has been thoroughly discussed and compared against the state of the art. Our analysis shows that FRODO is the only proposal that enjoys all the properties required to a secure micro-payment solution, while also introducing flexibility when considering the payment medium (types of digital coins). Finally, some open issues have been identified that are left as future work. In particular, we are investigating the possibility to allow digital change to be spent over multiple off-line transactions while maintaining the same level of security and usability.

REFERENCES

[1]. Vanesa Daza, Roberto Di Pietro, Flavio Lombardi, And Matteo Signorini "Frodo: Fraud Resilient Device For Off-Linmicro-Payments", Dependable And Secure Computing, IEEE Transactions On (Volume:PP , Issue: 99), 12 June 2015
[2]. R. L. Rivest, "Payword and micromint: two simple micropayment schemes," in CryptoBytes, 1996, pp. 69–87.
[3]. W. Chen,G. Hancke,K. Mayes,Y. Lien, and J.-H. Chiu,"Using 3G network components to enable NFC mobile transactions and authentication," in IEEE PIC '10, vol. 1, Dec 2010, pp. 441 –448.
[4]. T. Nishide and K. Sakurai, "Security of offline anonymous electronic cash systems against insider attacks by untrusted authorities revisited,"ser. INCOS'11.Washington, DC, USA: IEEE Comp. Soc., 2011, pp.656–661.
[5]. M. A. Salama, N. El-Bendary, and A. E. Hassanien, "Towards secure mobile agent based e-cash system," in Intl. Workshop on Security and Privacy Preserving in e-Societies. New York, NY, USA: ACM, 2011, pp. 1–6.
[6]. J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," ser. CHES '07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 63–80.
[7]. S. Gomzin, Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions, 1st ed. Wiley Publishing, 2014.
[8]. Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," SIAM J.Compute, vol. 38, no. 1, pp. 97–139, mar 2008.
[9]. B. Kori, P. Tuyls, and W. Ophey, "Robust key extraction from physical uncloneable functions," in Applied Cryptography and Network Security,ser. LNCS, J. Ioannidis, A. Keromytis, and M. Yung, Eds. Springer Berlin Heidelberg, 2005, vol. 3531, pp. 407–422.
[10]. M.-D. Yu, D. MRaihi, R. Sowell, and S. Devadas, "Lightweight and Secure PUF Key Storage Using Limits of Machine Learning," in CHES 2011, ser. LNCS, B. Preneel and T. Takagi, Eds. Springer Berlin Heidelberg, 2011, vol. 6917, pp. 358–373.
[11]. C. R. Group, "Alina & Other POS Malware," Cymru, Technical Report,2013.
[12]. N. Kiran and G. Kumar, "Reliable OSPM schema for secure transaction using mobile agent in micropayment system," in ICCCNT 2013, July 2013, pp. 1–6.
[13]. S. Gomzin, Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions, 1st ed. Wiley Publishing, 2014.
[14]. C. Wang, H. Sun, H. Zhang, and Z. Jin, "An improved off-line electronic cash scheme," in ICCIS 2013, June 2013, pp. 438–441.
[15]. C.-I. Fan, V. S.-M. Huang, and Y.-C. Yu, "User efficient recoverable off-line e-cash scheme with fast anonymity revoking," Mathematical and Computer Modelling, vol. 58, no. 12, pp. 227 – 237, 2013.
[16]. 1M.-D. Yu and S. Devadas, "Secure and robust error correction for physical unclonable functions," Design Test of Computers, IEEE, vol. 27, no. 1, pp. 48–65, Jan 2010.