International Journal of Computational Research and Development (IJCRD)
Impact Factor: 4.775, ISSN (Online): 2456 - 3137
(www.dvpublication.com) Volume 1, Issue 2, 2016

OFF-LINE MICRO PAYMENTS USING FRODO RESILIENT DEVICE

G. Kavipriya*, S. Senthilnathan & Dr. T. Senthil Prakash*****

* PG Scohar, Department of Computer Science and Engineering, Shree Venkateshwara Hi-Tech Engineering College, Gobi, Tamilnadu

** Assistant Professor, Department of Computer Science and Engineering, Shree Venkateshwara Hi-Tech Engineering College, Gobi, Tamilnadu

*** Professor & HOD, Department of Computer Science and Engineering, Shree Venkateshwara Hi-Tech Engineering College, Gobi, Tamilnadu

Cite This Article: G. Kavipriya, S. Senthilnathan & Dr. T. Senthil Prakash, "Off-Line Micro Payments Using FRoDO Resilient Device", International Journal of Computational Research and Development, Volume 1, Issue 2, Page Number 56-59, 2016.

Abstract:

Credit and debit card data theft is one of the earliest forms of cybercrime. Still, it is one of the most common nowadays. Attackers often aim at stealing such customer data by targeting the Point of Sale (for short, PoS) system, i.e. the point at which a retailer first acquires customer data. Modern PoS systems are powerful computers equipped with a card reader and running specialized software. Increasingly often, user devices are leveraged as input to the PoS. In these scenarios, malware that can steal card data as soon as they are read by the device has flourished. As such, in cases where customer and vendor are persistently or intermittently disconnected from the network, no secure on-line payment is possible. This paper describes FRoDO, a secure off-line micro-payment solution that is resilient to PoS data breaches. Our solution improves over up to date approaches in terms of flexibility and security. To the best of our knowledge, FRoDO is the first solution that can provide secure fully off-line payments while being resilient to all currently known PoS breaches. In particular, we detail FRoDO architecture, components, and protocols. Further, a thorough analysis of FRoDO functional and security properties is provided, showing its effectiveness and viability.

Key Words: Pos System, Cyber Crime & Micro-Payments

Introduction:

Network security consists of the policies and practices adopted to prevent and monitor access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals.

Over View:

Problems & Objectives:

The vendor have been victims of information security breaches and payment data theft targeting consumer payment card data and Personally Identifiable Information(PII).The user data can be used by the criminals for fraud operations. For improving security, the credit card and debit card holders use Payment card industry Security Standard Council. PoS system always handle critical information and requires remote management. PoS System acts as gateways and require network connection to work with external credit card processors. However, a network connection not be available due to either a temporary network service or due to permanent lack of network coverage. on solutions are not very efficient since remote communication can introduce delays in the payment process. Brute forcing rem in PoS intrusions.

Existing System:

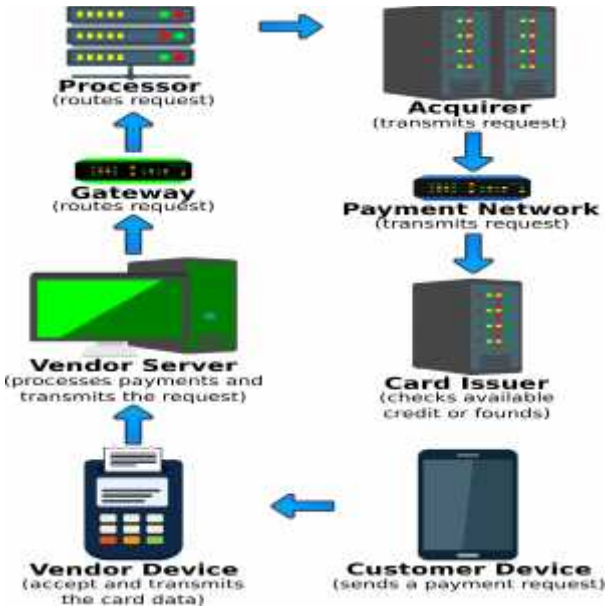
Mobile payment solutions proposed so far can classified as totally on-line semi off-line , weak off-line or totally off-line. The most issue with a totally off-line approach is that the problem of checking the trait of dealings whiles not a trusty third party. Keeping track of past transactions with 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.

Proposed System:

The Strong physical unclonable functions may perform any pre- computed challenge response pair. Physical unclonable every transistor in an integrated circuit has slightly different physical properties that lead to measurable differences in electronic properties. Process variations are not controllable during manufacturing; the physical properties of a device cannot be copied or cloned. As such, they are unique to that device and can be used for authentication purposes. The first solution that neither requires trusted third parties, nor bank accounts, nor trusted devices to provide resiliency against frauds based on data breaches in fully off-line

electronic payment systems. By allowing FRoDO customers to be free from having a bank account, makes it also particularly interesting as regards to privacy. Digital coins used in FRoDO are just a digital version of real cash and, as such, they are not linked to anybody else than the holder of both the identity and the coin element.

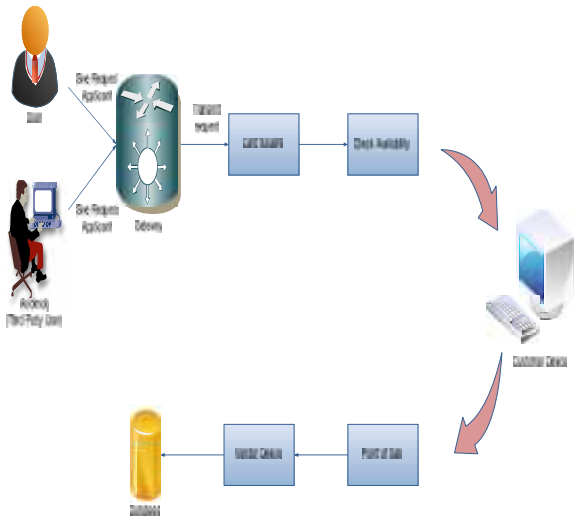
System Architecture:



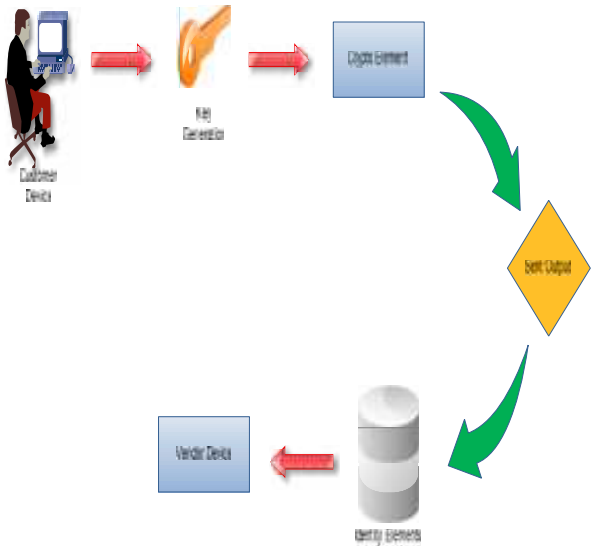
Module List:

- ✓ Client Module
- ✓ Key Generator
- ✓ Secure Payment
- ✓ Transaction At Coin Element
- ✓ Security Analysis

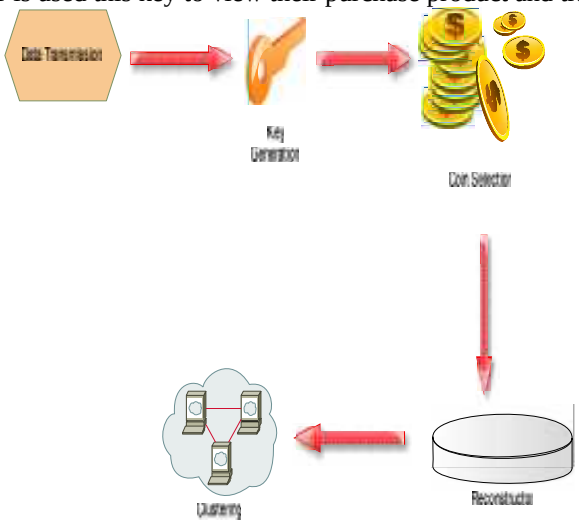
Client Module: This module used to client is going to online website. And View Product and select to product models and view product details. Select and purchase their product .and transaction from their account All details are encrypted by using Private Key and public key, Keys are generated during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



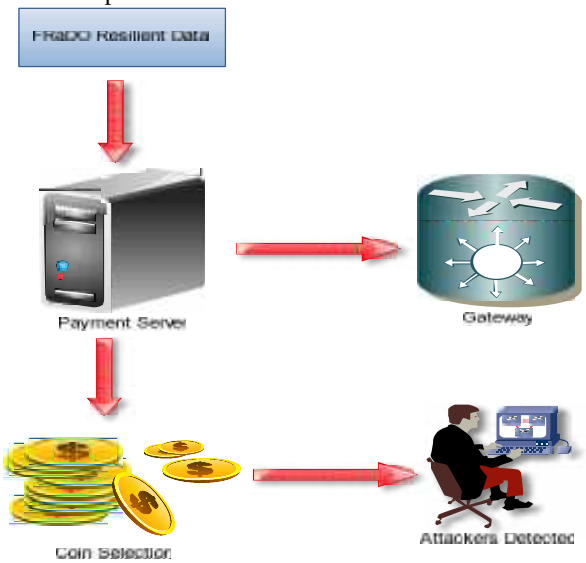
Key Generator: This module is using cryptographic algorithm, this algorithm used for symmetric and asymmetric cryptographic algorithms applied to received the data input and sent as output by the identity element. Key Generator is by PUFs, which have been used to implement strong challenge-response authentication. 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, warranty period, etc., and admin view all users purchase products but cannot view user account details. and to view which product is delivered or not.



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.

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 approaches.. Further, FRODO is also the first solution in the literature where no customer device data attacks can be exploited to compromise the system. Furthermore, our proposal has been thoroughly discussed and compared against the state of the art. 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. G. Kavipriya, S. Senthilnathan, Dr. T. Senthil Prakash, “Off-line Secure Credits for Micro Payments Using FRODO Resilent Device” Vol 4 Issue11 3221 5687, (P) 3221 568X, November2016.
2. 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
3. R. L. Rivest, “Payword and micromint: two simple micropayment schemes,” in Crypto Bytes, 1996, pp. 69–87.
4. 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.
5. 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.