Perspectives in Communication, Embedded-Systems and Signal-Processing (PiCES)
ISSN: 2566-932X, Vol. 1, Issue 5, August 2017
Proceedings of National Conference on Emerging Trends in VLSI, Embedded and Networking (NC-EVEN 17), May 2017 – Part 1

Offline Micro-Payment Recovers Fraud

Asha Rani S[1], Bhavana Sai B[1], Namrata S Bhat[1],Sanjay J[1],Shashidhar MS[2]

1. UG Students, Dept. of CSE, SRS Institute of Technology, Bengaluru, India.
2. Assistant Professor, Dept. of CSE, SRS Institute of Technology, Bengaluru, India.

Abstract: The payment of cash to products as it moved from cash to cashless which is of credit and debit cards. This mainly evolved in a problem these days .Due to this the customer data can be stolen by using of point of sale. Although the modern PoS are provided with stronger and managing the specialized software, it's difficult to prevent data theft although sophisticated securities are provided. Therefore by considering this situation secured online payment is not possible if the users are disconnected from the network. This paper implements the solution that provides fully secured offline micropayments where it highly recovers from cyber-attack. The hardware requirements, protocols and components are discussed in this paper. Further a complete description of offline micropayment functionality and provided with security property, which shows the productiveness and feasibility.

Keywords: Feasibility, Offline Micro-payment, Point of sale (PoS), Security.

I. INTRODUCTION

Gradually our Indian economy is progressing and we are switching to cashless payment which uses debit card and credit card. It is also replaced by mobile based payments. As the providence is developing, the fraud activities are also increased. To eradicate this we are implementing the solution which recovers the fraud by using offline micro-payments [3] that provides security and flexibility to the users.

II. PROBLEMS AND OBJECTIVES

The retail organizations have been victims for the information security payment data theft by targeting the PoS [2] which includes customer's payment card data. The data which is present in the credit and debit card will be used for the fraud operations, PoS [2] system will always handle the critical information of payment card data. The PoS system requires the network connection for the transaction process. Sometimes there is a lack of permanent network coverage and the other network services. These solutions are not sufficient for the secure payment process.

III. LITERATURE SURVEY

A. Secure Pos & Kiosk - Author: Bomgar

Limited interfaces and location within local networks, supporting kiosks and point of sale (POS) [2] terminals can be challenging. Often they are located on networks that are not connected to the internet, making direct access impossible for most remote support tools. And even when an employee is present at the terminal, access restrictions and/or lack of technical knowledge makes communicating the solution to a problem difficult. To add complications, hackers are ramping up their efforts to steal payment card data by gaining access to POS systems and kiosks.

B. Payword and micro mint: two simple micropayment schemes – Author: R. L. Rivest

The Basic Peppercorn method can be implemented in a variety of ways, to maximize ease of use for the customer in a given situation. While the basic pepper coin method requires that each consumer have digital signature capability, one can easily eliminate this requirement by having a party trusted by the consumer sign payments for him as a proxy; this might be a natural approach in a web services environment.

The pepper coin method can also be implemented so that it feels to the consumer as a natural extension of his existing credit-card processing procedure, further increasing consumer acceptance and ease of use.

C. Reliable OSPM schema for secure transaction using mobile agent in micropayment system - Author: NC Kiran

The paper introduces a novel offline payment system in mobile commerce using the case study of micro-payments. The present paper is an extension version of our prior study addressing on implication of secure micropayment system deploying process oriented structural design in mobile network. The previous system has broad utilization of SPKI and hash chaining to furnish reliable and secure offline transaction in mobile commerce. However, the current work has attempted to provide much more light weight secure offline payment system in micro-payments by designing a new schema termed as Offline Secure Payment in Mobile Commerce (OSPM). The empirical operations are carried out on three types of transaction process considering maximum scenario of real time offline cases. Therefore, the current idea introduces two new parameters i.e. mobile agent and mobile token that can ensure better security and comparatively less network overhead.

IV. RELATED WORK

The Mobile wallet solutions established so far are said to be fully online or semi offline the main problem with the fully offline payment is checking of truthfulness of payment without any third party. This is the main reason

NC-EVEN was held at Brindavan College of Engineering, Bengaluru, India on 11th May, 2017.

in the recent couple of years, many researchers on offline payment are said to be reliable and it is very important to consider, our previous work FROCE which is very similar to offline micro-payments [3] that is built using PUF architecture although several works have been introduced on the offline payments but this paper overcomes the limitations and brings further improvements.

V. PROPOSED SOLUTION

The solution given in this paper mainly describes the offline micropayment based on a feasible PUF functionality .PUF [4] is a concept which was said to be introduced in year 2001 by Ravikanth. The main physical property of this cannot create any duplication and these cannot be used for authentication process. Compare to other solutions the offline micropayment is said to be dabbled hardware. Where digital coins used in offline micropayments are said to be of digital version of the absolute cash, which cannot be linked to anything except the identity element and coin element [1].

Furthermore it is important to highlight that offline micropayments are secured and reliably hides some of the digital coins. Offline micropayments does not require any hardware component expect the coin element and identity element[1] which can be either stoppled into the customer device or directly fixed into the device .this paper is the first solution that doesn't require any third party bank accounts or trusted devices to recover from the attacks.

VI. SYSTEM DESIGN

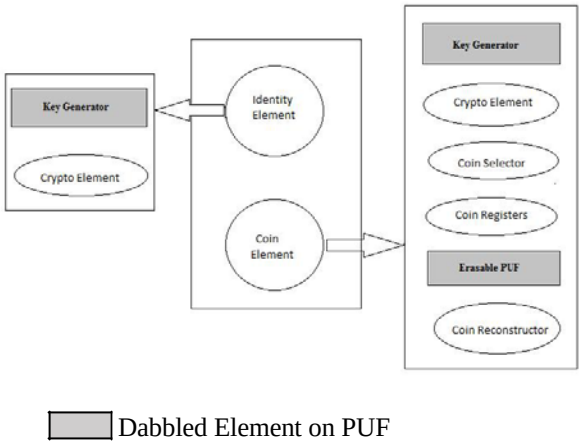

Fig 1. System Architecture

A. *Identity element:*

- *Key Generator*: It is used to check the progress of the process.
- *Crypto Element:* It is used for symmetric and asymmetric cryptographic algorithm to the received input and send as output by the identity element.

B. *Coin Element:*

- *Key Generator*: It is used to check the progress of the process.
- *Crypto Element*: It is used for symmetric and asymmetric cryptographic algorithm to the received input and send as output by the coin element.
- *Coin selector*: It is used to select the correct registers in order to obtain the final coin value
- *Coin register*: It is the one which stores both the PUF input and output values require rebuilding the original values.
- *Erasable PUF:* Even if the input is simple the output is of random
- *Coin Reconstrutor*: The reconstrutor [5] uses the helper data in coin register to remove the original output from the PUF [4].

Coin element and the Identity Element [1] are built on the Physical unclonable function (PUF). Both consist of same properties

- Clone: It is very hard to clone a strong PUF
- Emulation: Due to a very Large Number Of challenge in the PUF it is very hard to emulate the data.
- Unpredictable: it is very difficult to predict the request of a PUF due to a random Selection of challenge

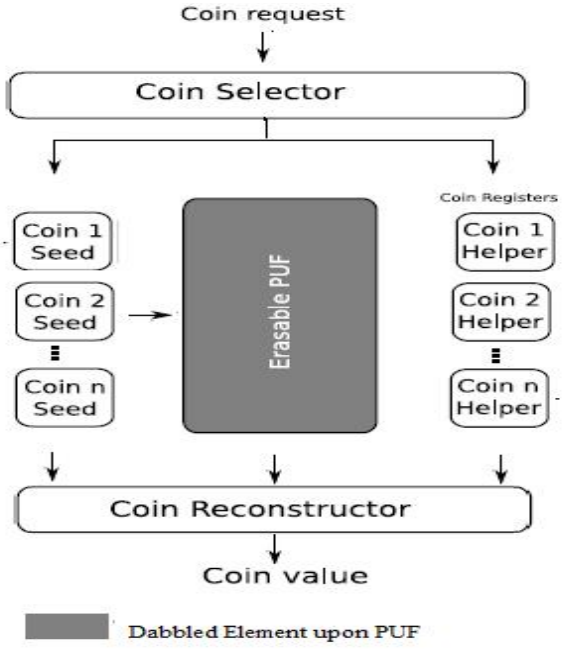

Fig 2. Coin Reconstruction based on PUF

Fig 2 shows how the coin will be reconstructed [5] .The user and the vendor does not contain the erasable-PUF challenge by themselves. The coin request will be given as input to the coin selector. The coin selector will select the coin registers that involved in the transaction. The selected coin register will be used as input to the erasable-PUF .the coin helper register is combined with

the PUF output to reconstruct the original value of the coin.

VII. Conclusion And Future Work

In this paper we have established offline micropayment as the first solution for fully secured offline micropayments, and the security analysis also says that it doesn't require any third party or truthful assumptions. Our analysis shows that offline micropayment is the only one with the secured micropayment solution .finally there is said to some issues detected that is kept for future work .then in particularly we are checking with many multiple offline transaction which stays with same level of confidentiality and usability.

REFERENCES

[1] Shana Jebin P, "Payoff: An approach for Offline micro-Payments," Coin element and Identity element, DOI: 10.15680/IJIRCCE.2017.0503107, Vol. 5, Issue 3 March 2017.

[2] R. Bargavi, Dr. L. Jaba Sheela, "Fraud Resilient Device Offline Micro-Payments using Bit-Exchange Algorithms, "Point of Sale, 58.10 DOI: 10.18535/ijecs/v6i3.54, Volume 6 Issue 3 MARCH, 2017Page No. 20699-20704

[3] R. Siva Kumar, V. Hemalatha, M. Mugila, L. Mythili," Fraud Resilient Device for Off-Line Micro Payments, "Secure fully off-line micro-payments, International journal of Engineering science and Computing, ISSN XXXX XXXX © 2017 IJESC Volume 7 Issue No.3 March 2017.

[4] G.Kavipriya.M E,S.Senthilnathan ME,Dr. T. Senthil Prakash,"OFF-Line Secure Credits For Micro Payments Using FRoDO Resilient Devices,"Physical Unclonable Function,IJOSER Vol 4 Issue 11 November-2016.

[5] Vanesa Daza, Roberto Di Pietro, Flavio Lombardi, and Matteo Signorini,"FRoDO: Fraud Resilient Device for Off-Line Micro-Payments,"Coin Reconstrutor, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 13, NO. 2, MARCH/APRIL 2016