ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

A Survey on Secure Off-Line Payment Solution for Physical Unclonable Functions

Namitha J[1], Bhavya Shree J[2], Santhosh N[3], Kiran Kumar N[4], Himabindu U[5]

B.E Student (8th semester), Dept. of Computer Science and Engineering, Jnanavikas Institute of Technology, Bidadi, India[1,2,3,4]

Assistant Professor, Dept. of Computer Science and Engineering, Jnanavikas Institute of Technology, Bidadi, India.[5]

ABSTRACT: An online threat has been increasing due to the use of credit card and pos services. The customer data is got by consumer at this point of POS. A malware can be added to the pos device or a fault chip can be inserted into the POS to capture the customer details. This is a threat this can be overcome by considering the payment as offline. Here we present a offline model called OFFLINE MODEL that will be offline and payments will be through offline generating digital coins. This increases security in the payments.

KEYWORDS: POS, OFFLINE MODEL, digital coins

I.INTRODUCTION

Showcase experts have anticipated that versatile instalments will over-take the customary market, in giving more prominent comfort to buyers and new wellsprings of income to many organizations. This situation delivers a move in buy techniques from great MasterCard's to new methodologies, for example, versatile based instalments, giving new market players novel business possibilities. Comprehensively bolstered by late equipment, portable instalment innovation is still at its initial phases of improvement yet it is relied upon to ascend sooner rather than later as exhibited by the developing enthusiasm for crypto-monetary forms.

Despite the fact that PoS bursts are declining, regardless they remain an to a great degree satisfying attempt for lawbreakers. Client information can be utilized by cybercriminals for fake operations, and this offline module the instalment card industry security benchmarks committee to set up information security measures for each one of those associations that handle credit, charge and ATM cardholder data.

Regardless of the structure of the electronic instalment framework, PoS frameworks dependably handle intense data and, as a rule, they likewise require remote administration. PoS frameworks go about as entryways and require a few kind of system association keeping in mind the end goal to contact outside Visa processors. This is obligatory to verify exchanges. In any case, bigger organizations that desire to tie their PoS's with other back-end frameworks may associate the
previous to their own inside systems.

II.RELATED WORK

Versatile instalment arrangements proposed so far can be characterized as completely on-line [8], [9], [10], [11], semi disconnected [12], [13], frail disconnected [14], [15] or completely disconnected [16], [17], [18]. The principle issue with a completely disconnected approach is the trouble of checking the reliability of an exchange without a trusted outsider. Truth be told, monitoring past transactions with no accessible association with outer gatherings or shared databases can be very troublesome, as it is troublesome for a Exchange Attack/ Aggressor M.
Seller to check if some advanced coins have as of now been spent. This is the primary motivation behind why amid most recent couple of years, a wide range of methodologies have been proposed to give a solid disconnected instalment plot. Albeit many works have been distributed, they all centered around exchange anonymity and coin unforgeability.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

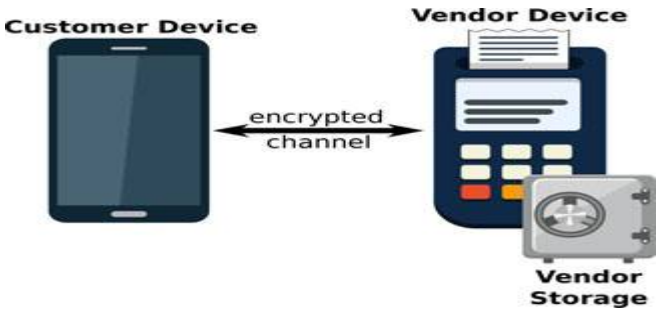
In any case, past solutions do not have an intensive security investigation. While they concentrate on hypothetical assaults, dialog on genuine assaults, for example, skimmers, scrubbers and information vulnerabilities is absent. As respects physical unclonable capacities [19], a key com- ponent of our answer, different applications on managing an account scenarios have as of now been proposed in the past [20]. This is an inward aggressor with finish access to all the included gadgets. As for PoS information vulnerabilities, there are three particular assaults that must be investigated:
case such solid capacities are by and large utilized for verification purposes as it were. All things considered, they just assurance that information has been figured on the correct gadget yet they can't give any evidence about the dependability of the information itself.

III.THREATS

In light of the abilities and on the measure of gadgets that can be gotten to amid the assault, a scientific categorization of the aggressors is first presented as takes after:
Authority. This is an outer assailant ready to overhang offline model and modify messages being traded between the client and the merchant gadget;
Pernicious client. (M. Client) this is an inside assailant that can either physically open the client gadget to listen in delicate data or infuse pernicious code inside the client gadget all together to modify its conduct;
Vindictive seller. (M. Merchant) it is an inside assailant that can either listen in data from the merchant gadget or infuse pernicious code in it in request to adjust its conduct;
Information in memory. The objective of this assault is card information that is sustain into the PoS framework by some info gadget. One approach to maintain a strategic distance from such assault is by encode ing the card information at the earliest opportunity and by keeping it scrambled to the extent that this would be possible through its life inside the framework;
Data in travel. The objective of this assault is the information that is traded between every one of the substances of the sys- tem that procedures client's information. Indeed, even in completely off-
line electronic instalment frameworks, this assault is still accessible. Truth be told, an instalment framework is normally com-postured by at least two components and card information is traded between every one of them. The advances that are ordinarily utilized for tending to the information in travel weakness incorporate SSL, TLS and, IPsec [21];
Data very still. The objective of this assault is the card information put away in non-unpredictable recollections inside the framework. The best way to maintain a strategic distance from such sort of assault is to dodge any information stockpiling whatsoever [21].

IV.OFFLINE MODEL

The offline modelis mainly based on the concept of Utility function.



Using offline model we create an encrypted channel between customer device and vendor device. Here the authentication of vendor is done by utility function, and a common agreement should be between vendor and user. Coin element is generated randomly instead of real cash. Here utility function is master of offline model model.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

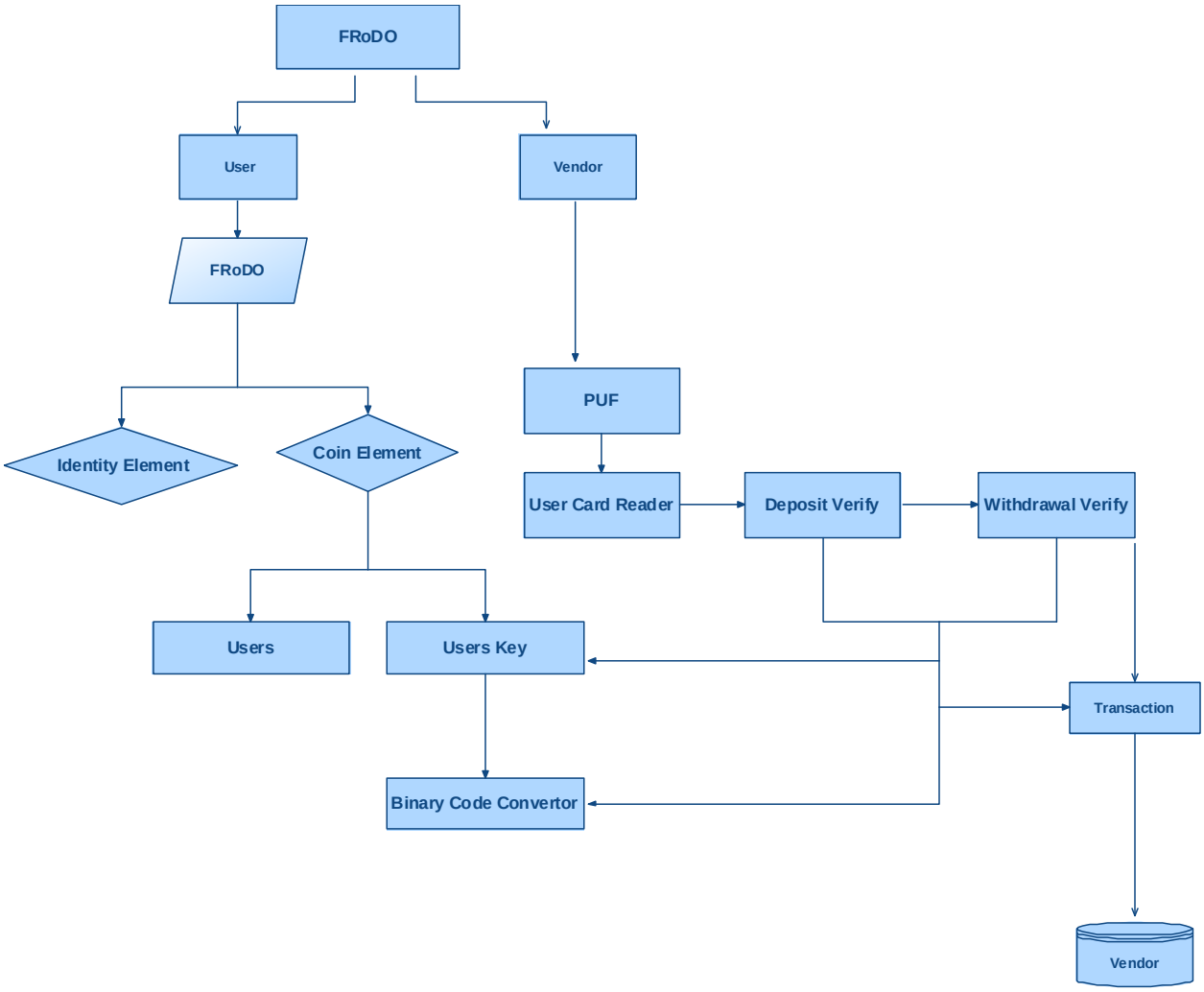


Fig.2 Architecture of offline model

Working: The above diagram shows the architecture of offline model with two entities i) user ii) Vendor Where identity element will authenticate the user, Puf will authenticate the depositor. Now both User and vendor should register with common bank. The coin is generated for the card number and the money will be deposited based on coins generated in authentication with the Puf.

V.CONCLUSION

The increase in online thefts is increasing to avoid that we have developed architecture of the offline model. Here there will be a double authentication for login as well as for payment. further extension of implementing the above architecture in cloud environment and checking its performance.

REFERENCES

1. C.-L. Chen and J.-J. Liao, "Fair offline digital content transaction system," IET Inf. Security, vol. 6, no. 3, pp. 123–130, Sep. 2012
2. C.-I. Fan, V. S.-M. Huang, and Y.-C. Yu, "User efficient recoverable off-line e-cash scheme with fast anonymity revoking," Math. Comput.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Model. vol. 58, no. 12, pp. 227–237, 2013.

3. J. Liu, J. Liu, and X. Qiu, "A proxy blind signature scheme and an off-line electronic cash scheme," Wuhan Univ. J. Natural Sci., vol. 18, no. 2, pp. 117–125, 2013.
4. M.-D. Yu and S. Devadas, "Secure and robust error correction for physical unclonable functions," IEEE Design Test Comput., vol. 27, no. 1, pp. 48–65, Jan. 2010.
5. W. Chen, G. Hancke, K. Mayes, Y. Lien, and J.-H. Chiu, "Using 3G network components to enable NFC mobile transactions and authentication," in Proc. IEEE Int. Conf. Progress Informat. Comput., Dec. 2010, vol. 1, pp. 441–448.
6. M.-D. Yu, D. MRaihi, R. Sowell, and S. Devadas, "Lightweight and secure PUF key storage using limits of machine learning," in Proc. Int. Workshop Cryptographic Hardware Embedded Syst., 2011, vol. 6917, pp. 358–373.
7. V. C. Sekhar and S. Mrudula, "A complete secure customer centric anonymous payment in a digital ecosystem," in Proc. Int. Conf. Comput., Electron. Elect. Technol., 2012, pp. 1049–1054.
8. S. Dominikus and M. Aigner, "mCoupons: An application for near field communication (NFC)," in Proc. 21st Int. Conf. Adv. Inf. Netw. Appl. Workshops, 2007, pp. 421–428.
9. T. Nishide and K. Sakurai, "Security of offline anonymous electronic cash systems against insider attacks by untrusted authorities revisited," in Proc. 3rd Int. Conf. Intell. Netw. Collaborative Syst.,2011, pp. 656–661.
10. W.-S. Juang, "An efficient and practical fair buyer-anonymity exchange scheme using bilinear pairings," in Proc. 8th Asia Joint Conf. Inf. Security, Jul. 2013, pp. 19–26.
11. M. A. Salama, N. El-Bendary, and A. E. Hassanien, "Towards secure mobile agent based e-cash system," in Proc. Int. Workshop Security Privacy Preserving e-Soc., 2011, pp. 1–6.
12. C. Wang, H. Sun, H. Zhang, and Z. Jin, "An improved off-line electronic cash scheme," in Proc. 5th Int. Conf. Comput. Inf. Sci., Jun. 2013, pp. 438–441.
13. J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in Proc. 9th Int. Workshop Cryptographic Hardware Embedded Syst., 2007, pp. 63–80.
14. R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical oneway functions," Science, vol. 297, no. 5589, pp. 2026–2030, 2002.
15. S. Gomzin, Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions, 1st ed. New York, NY, USA: Wiley, 2014.