International Journal of Advanced Scientific Technologies ,Engineering and Management Sciences (IJASTEMS-ISSN: 2454-356X) Volume.3,Special Issue.1,March.2017

Impact For Reducing Digital Attacks In Point Of Sales Terminal Transactions

B.J. Annie Neeraja[11,]University Computer Center, SPMVB, Tirupathi

Email: annie.neeraja@gmail.com

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. As the usage of Credit Card, Debit Card and Internet Banking as Increased, all business and other transactions are digital but also we find 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 off-line payment. The 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 Coin details at customer side and automatically erases after the transaction. It include that limited activity is ensured referred as server to client transaction is secured. Further, an exhaustive investigation of Digital Security utilitarian and security properties is given, demonstrating its viability and plausibility. As an exhaustive extension to the project further investigated with possibility to allow digital change to be spent over multiple off-line transactions while maintaining the same level of security and usability. Providing an exhaustive Coin Management in framing and creating On Mobile Move Coins.

Index Terms- Digital secure payment, Architecture, protocols, cybercrime, Security for Digital Attacks.

1. INTRODUCTION

Credit and debit card data stealing is most popular problem in cybercrime. Slashers aim at stealing the customer data by aiming the Point of Sale systems, i.e. the point at which the vendor handle the customers data. Modern POS systems having specialized software inbuilt in card reader. Often user devices are external input to the POS. In these concepts, malware steal the card data should read by device has proliferated. Like this situation, connection between customer and vendor being intermediately stopped and there secure on-line payment is not possible. This projects providing Digital Security concepts for a secure off-line micro-payment is flexible to POS data breaches.

Solution includes flexibility and security. Still, Digital Security is the first solution that can provide fully secure off-line payments while being flexible to all currently known POS failures. In certain, it include Digital Security architecture, components, and protocols. Thereby, a complete details of Digital Security functional, security properties are provided, showing its effectiveness and viability. Mobile micro payments are famous and they are traditional in marketing fields. The classic credit card approaches may be implemented in banking such as mobile-based payments. Even though many technologies developed, many unexpected problems faced in the field for that the crypt-currencies and de-centralized payment systems are used. Due to several unresolved problems, including a lack of widely-accepted standards, limited interoperability among systems and security the payment schemes are not get successful in the payment system.

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.

The Digital Security introduces a secure off physical unclonable function. Digital Security introduces coin element and identity element. Vendor only communicate with the identity to identify the user. Identity element I the security of users. Market analysts have predicted that mobile payments will overtake the traditional marketplace, thus providing greater convenience to consumers and new sources of revenue to many companies. This scenario produces a shift in purchase methods from classic credit cards to new approaches such as mobile-based payments, giving new market entrants novel business chances. Widely supported by recent hardware, mobile payment technology is still at its early stages of evolution but it is expected to rise in the near future as demonstrated by the growing interest in crypto-currencies,

The main benefit is a simpler, faster, and more secure interaction between the involved actors/entities. Among other properties, this two-steps protocol allows the bank or the coin element issuer to design digital coins to be read only by a certain identity element, i.e., by a specific user. Furthermore, the identity element used to improve the security of the users can also be used to thwart malicious users. In proposed solution that can provide secure fully off-line payments while being resilient to all currently known PoS breaches.

II.RELATED WORK

Most of the payment transactions are processed by an electronic payment system(EPS). The EPS and PoS are located in same machine, where PoS is a tool used by cashier or consumer, while EPS performs all payment processing.

III.METHODOLOGY

In the present method, the approach describes Digital Security, a at ease off-line micro-cost solution that's resilient to PoS information breaches. Digital Security presents a constant structure in developing and preservation of coins. The Digital Security solution cannot improves over up to the moment procedures in phrases of flexibility and protection required by using user. The Digital Security introduces a cozy off bodily function. Digital Security introduces coin detail which are static in nature and can't be converted on move or on Requirement. In detailed present Digital Security structure, components, and protocols does now not supplies effectiveness and viability.

The system implemented called Digital Security, was built using a static coin architecture which are easier to hack.

Current Digital Security Does not provides Coins Management.

Digital Security is a weak prevention strategy based on data obfuscation and did not address the most relevant attacks aimed at threatening customer sensitive data, thus being vulnerable to many advanced attack techniques.

IV. PROPOSED WORK

Project is proposed with advanced investigation and possibility to allow extensive digital change to be spent over multiple off-line transactions while maintaining the same level of security and usability. Project can be extended with Coin Management in framing and creating On Mobile Move Coins. Project is extended with UmcDigital Security (User Management of Coins with Fraud Resilient Device for Off-line micro-Payments). Extended Digital Security provides coin management as need of user requirements.

The system Extended with UMC Digital Security, with a changed architecture for user coin management.

UMDigital Security provides On Mobile Coins Management.

UMDigital Security is provides prevention strategy based on data obfuscation and address the most relevant attacks aimed at threatening customer sensitive data, thus being vulnerable to many advanced attack techniques.

Creating on Mobile Coins provides user in generating and managing coins when needed.

V.MODULES AND IMPLEMENTATION

System Construction Module

In the first module, develop the System Construction module with the various entities: Vendor, User, Digital Security, PUF, Attacker. This process is developed completely on Offline Transaction process. Develop the system with user entity initially. The options are available for a new user to register first and then login for authentication process. Then develop the option of making the Vendor Registration, such that, the new vendor should register first and then login the system for authentication process. Digital Security is 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 a fully off-line electronic payment systems. Furthermore, by allowing Digital Security customers to be free from having a bank account, makes it also particularly interesting as regards to privacy. In fact, digital coins used in Digital Security 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. Differently from other payment solutions based on tamper-proof hardware, Digital Security assumes that only the chips built upon PUFs can take advantage from the tamper evidence feature. As a consequence project assumptions are much less restrictive than other approaches.

Identity Element

In this module, develop the Identity Element module functionalities. Digital Security does not require any special hardware component apart from the identity and the coin element that can be either plugged into the customer device or directly embedded into the device. Similarly to secure elements, both the identity and the coin element can be considered tamperproof devices with a secure storage and execution environment for sensitive data. Thus, as defined in the ISO7816-4 standard, both of them can be accessed via some APIs while maintaining the desired security and privacy level. Such software components (i.e., APIs) are not central to the security of solution and can be easily and constantly updated. This renders infrastructure maintenance easier.

Coin Element

In this module, develop Coin Element. In this coin Element develop Key Generator and Cryptographic Element. The Key Generator is used to compute on-the-fly the private key of the coin element. The Cryptographic Element used for symmetric and asymmetric cryptographic algorithms applied to data received in input and send as output by the coin element; The Coin Selector is responsible for the selection of the right registers used together with the output value computed by the coin element PUF in order to obtain the final coin value; The Coin Registers used to store both PUF input and output values required to reconstruct original coin values. Coin registers contain coin seed and coin helper data.

Attack Mitigation

In this module develop the Attack Mitigation process. The read-once property of the erasable PUF used in this solution prevents an attacker from computing the same coin twice. Even if a malicious customer creates a fake vendor device and reads all the coins, it will not be able to spend any of these coins due to the inability to decrypt the request of other vendors. The private keys of both the identity and coin elements are needed to decrypt the request of the vendor and can be computed only within the customer device. The fake vendor could then try to forge a new emulated identity/coin element with private/ public key pair. However, identity/coin element public keys are valid only if signed by the bank. As such, any message received by an unconfirmed identity/coin element will be immediately

rejected; Each coin is encrypted by either the bank or the coin element issuer and thus it is not possible for an attacker to forge new coins

VI. CONCLUSION AND FUTURE SCOPE

In this paper, we discussed the proposed analytical architecture of real time big data for remote sensing applications. The proposed architecture is designed in such a way that; it can analyze both the offline as well as the real time data in an efficient way. In this paper, we discuss architecture for real-time Big Data analysis for remote sensing application. The Remote sensing Big Data architecture efficiently processed and analyzed real-time and offline remote sensing Big Data for decision-making. The proposed architecture is contains three major units, such as 1) RSDU; 2) DPU; and 3)DADU. These units implement algorithms for each level of the architecture depending on the required analysis. The architecture of real-time Big is generic (application independent) that is used for any type of remote sensing Big Data analysis. Furthermore, the capabilities of filtering, dividing, and parallel processing of only useful information are performed by discarding all other extra data. These processes make a better choice for real-time remote sensing Big Data analysis. The Remote Sensing Big Data architecture welcomes researchers and organizations for any type of remote sensory Big Data analysis by developing algorithms for each level of the rchitecture depending on their analysis requirement. For future work, we are planning to extend the proposed architecture to make it suitable for Big Data analysis for all applications, e.g., sensors and social networking. We are also planning to use the proposed

architecture to perform complex analysis on earth observatory data for decision making at real-time, such as earthquake prediction, Tsunami prediction, fire detection, etc.

REFERENCES

[1] Vanesa Daza, Roberto Di Pietro, Flavio Lombardi, and Matteo Signorini: "Fraud Resilient Device for Off-Line Micro-Payments," in Ieee Transactions On Dependable And Secure Computing, Vol. 13, No. 2, March/April 2016.

[2] J. Lewandowska. (2013). [Online]. Available: http://www.frost.com/prod/servlet/press-release.pag?docid=274238535

[3] R. L. Rivest, "Payword and micromint: Two simple micropayment schemes," in Proc. Int. Workshop Security Protocols, 1996, pp. 69–87.

[4] S. Martins and Y. Yang, "Introduction to bitcoins: A pseudoanonymous electronic currency system," in Proc. Conf. Center Adv. Stud. Collaborative Res., 2011, pp. 349–350.

[5] Verizon, "2014 data breach investigations report," Verizon, Tech. Rep., 2014, http://www.verizonenterprise.com/DBIR/2014/

[6] T. Micro, "Point-of-sale system breaches, threats to the retail and hospitality industries," University of Zurich, Department of Informatics, 2010.

[7] Mandiant, "Beyond the breach," Mandiant, 2014, https://dl.mandiant. com/EE/library/ WP_M-Trends2014_140409.pdf.