International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 5 | ISSN : 2456-3307

Secure Digital Cash Payment through Coin Management

C. Jaya Prakash
M. Tech (SE), Department of CSE, JNTUCEA, Anantapur, Andhra Pradesh, India

ABSTRACT

Cybercrime is the most popular crimes in the recent times. Cybercrime involves theft of credit card and debit card information details and utilizing those credentials for various fraud operations. Security has been the main concern since decades. Due to the static implementation of the personal identification information there are novel chances of attacking the data by an attacker. Mainly the cybercrimes are observed in point of sale (POS) systems. The attackers aim to steal the customer details by infecting the point of sale systems with the malwares and these systems are equipped with a microprocessor and storage capacity to store the customer's card data. In the proposed method one can create dynamic coins and flying coins which reduces data masking and increases the security level. Flexibility will be achieved by implementing dynamic coins and flying coins.

Keywords: Cybercrime, Security, Credentials, Malwares, Microprocessor

I. INTRODUCTION

The main aim of the proposed system is to increase the level of security. Normally when we visit a shop or purchasing any item through online shopping we process the payment through credit cards and debit cards. The retailer uses point of sale systems to process the transaction and these devices are purchased by the retailers from the vendors. The attacker tends to steal the customer card details by infecting a malware into the point of sale systems. The point of sale systems acts as gateway and requires some sort of network connection in order to validate the transaction. To process the transaction one needs personal identification number (PIN). As these PIN number is static there are more chances to steal the card data as soon as the customer card details are read by the point of sale devices. In the proposed method we introduce dynamic coins and flying coins in order to validate the transactions. By using these type of coins in the transactions security level will be increased. The coins will be utilized only once and the coins will gets expired after usage. Dynamic coins are generated automatically and no need to enter manually. The flying coins are generated based on the requirement. To reduce the amount of cost and simplify administration and maintenance Point-of-Sale devices may be remotely managed over the internal networks.

II. LITERATURE SURVEY

Many point-of-sale terminals are manufactured using embedded versions of Microsoft windows [1]. The point-of-sale terminals are connected using a closed Wi-Fi network, the attacker nonetheless be able to crack its password [2].The intruders will find a solution to breach the servers which holds responsible for the Point-of-Sale information [3]. Point-of-Sale malware exploits this by capturing the payment card information directly from memory which is known as "RAM SCRAPPING". We can secure Point-of-Sale devices by limiting the access to the internet, routinely deleting the card holder data, deploying the latest version of operating system with updated patches and enforcing policies regarding the physical repair and upgrade of Point-of-Sale device.

V.C. Sekhar and S. Mrudula proposed a secure customer centric mobile payment scenario in which the merchant is disconnected from the acquirer due to lack of internet connection and still can be used for mobile transaction. A general account based payment model involves 4 parties. Card holder, Merchant, Issuer, and the acquirer [4]. The complete payment system is operated by payment system provider who maintains a relationship with banks [5].

III. EXISTING SYSTEM

Vanesa Daza, Roberto Di Pietro,Flavio Lombardi and Matteo Signorini introduces a micro payment approach, FRODO which uses multiple physical unclonable functions. It uses mainly two elements in order to process the transaction, identity element and the coin element [6]. The identity element is used to authenticate the user and the coin element which is used to authorize the transaction. Keeping track of past transactions becomes difficult with no available connection to external parties or databases [8]. It is difficult for vendor to check the past transactions (history) without a reliable connection. Most of the point of sale systems gets infected with malwares near vendors and it is mandatory to check repeatedly whether the device works perfectly or not [7]. There might be a chance of infecting the point of sale systems if the point of sale systems and the customers are connected to the same network. So the retailers have to maintain a separate connection in order to avoid all the hurdles.

IV. PROPOSED SYSTEM

In the proposed system we will be using coins concept to process the transaction. Different types of coins will be available in the market now-a-days. In the proposed method we will be utilizing static coin, dynamic coin, and the flying coin. Static coin is fixed, once we create a static coin it will be utilized N number of times and there is no restriction on the utilization of these types of coins. Dynamic coins gets changes each and every time. Once we utilize these coin the coin will gets expired and the user will be notified which coins are utilized. During the coins creation the user will be notified by using a short message service to the registered mobile number. Which coins are created and how many coins are created will be sent as short message service to the registered mobile number. Flying coins are generated upon request from the customer and can be utilized when needed. By utilizing these type of coins security level will be increased and flexibility will be achieved.

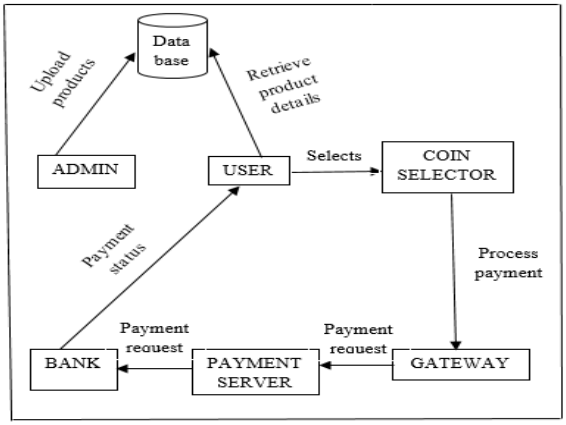

Figure 1: Block Diagram

We will be utilizing all these coins in the shopping zone. Generally when we visit a shop or purchasing any items from online shopping then we process the payment through different types of strategies. We process the payment in a shop by swiping our credit card and debit cards and entering our personal identification number to process the transaction successfully. While shopping online we process the payment by using different wallets, mobile based payments and so on.

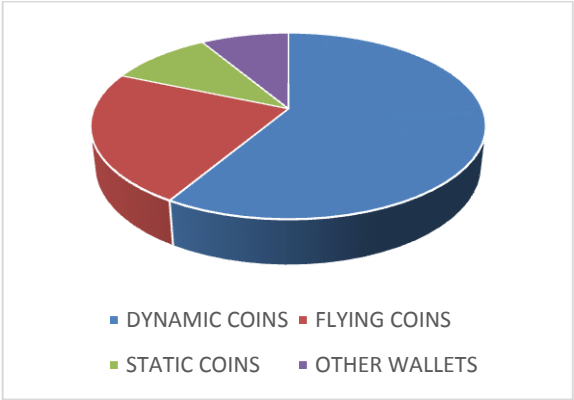

Figure 2: Payment Strategies

We process the transaction by using static pin numbers and thus creating a scope for the attacker or the intruder to modify the data and utilize it for various operations. In the proposed system we have different modules. Card owner, coins generation, admin module, and the client module. Card owner holds the responsibility of updating the coins irrespective of what type of coin it is. Coins generation is responsible for generating the coins and it is done by using a random number system algorithm. The random number system algorithm generates the dynamic keys which holds a major security feature in the proposed system. In the admin module, admin holds the responsibility of updating the

product details and the related information of the project such as cost of the project, quantity available, and name of the project. In the client module, the client makes usage to the products through authorized credentials. The client needs to register his or her mobile number while registration and any further updates will be sent to the registered mobile number. After selection of all the products the client needs to make the payment and the payment can be processed by using the credit card and debit card information details. While processing the transaction the client will be able to utilize different types of coins upon availability.

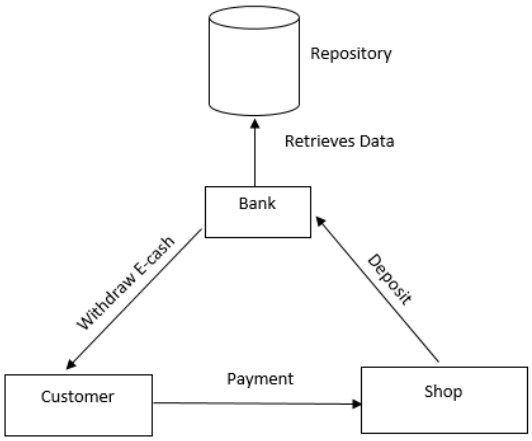

Figure 3: Flow in Electronic Cash System

When the transaction gets successfully completed then the user will be notified by using a short message service that which coin is utilized and what type of coin is utilized.

V. RESULTS

In the proposed system we will be having a web portal which consists of admin page and the client page. In the admin page the admin will be able to update all the information about the project. In the client page the client will be able to utilize all the resources made available by the admin and he will be able to process the payment by using different types of coins upon requirement.

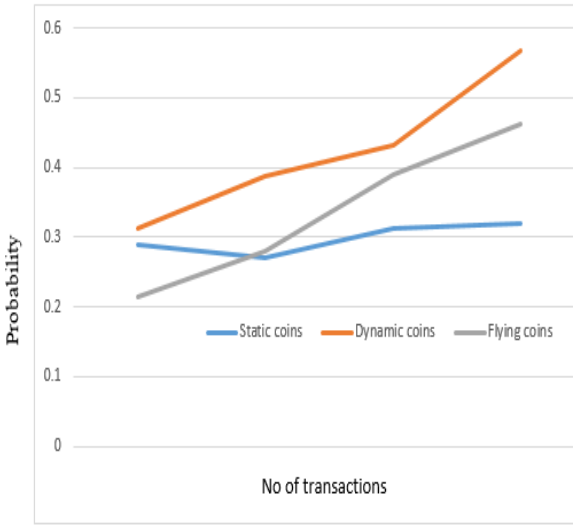

Figure 4: probability of usage of coins

The probability of usage of the dynamic coins and the flying coins will be high when compared to the static coins. The usage of the dynamic coins will provide more flexibility to process the payment transactions. Vulnerability is the main factor for which cyber-attacks are done. The implementation of the dynamic coins and flying coins results in more efficiency and it's free from several threats. During the transaction process the denial of service attacks becomes less by using the dynamic coins and flying coins.

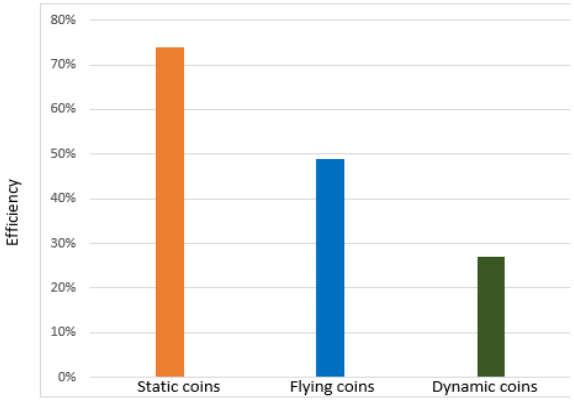

Figure 5: Efficiency based on Vulnerability factor

While performing the transaction delay occurs frequently and these delay is reduced with the usage of dynamic coins. Denial of service attacks reduces as the implementation of dynamic coins is processed.

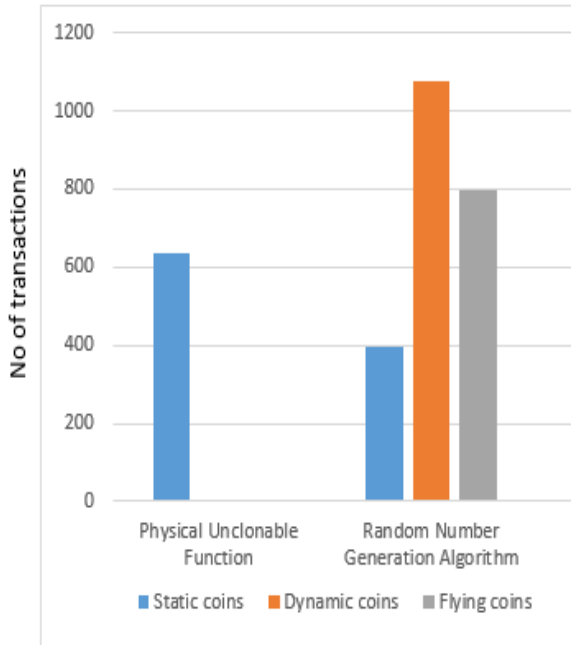

Figure 6: Comparison of used Functions

VI. CONCLUSION

We introduced coins management concept in this paper which adds more security for the clients debit card and credit card information details and make sure that they are utilized in a proper way. The processing of the transaction will become more effective and efficient. Delay gets reduced with the usage of Dynamic coins.

VII. REFERENCES

[1]. Bomgar, "Secure POS & kiosk support," Bogmar,2014,"https://www.bomgar.com/assets/documents/Bomgar_Remote_Support_for_POS_Systems.pdf

[2]. Verizon, "2014 data breach investigation report," Verizon, The. Rep., 2014,http://www.verizonenterprose.com/DBIR/2014/

[3]. 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.

[4]. V. Ahuja, Secure Commerce on the Internet, AcademicPress, 1996.

[5]. G. Horn and B. Preneel, Authentication and Payment in Future Mobile Systems, Proceedings of 5th ESORICS'98, Belgium, 1998, pp. 277-293.

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

[7]. https://en.wikipedia.org/wiki/Physical_unclonable_function

[8]. G. Vasco, Maribel, S. Heidarvand and J. Villar, " Anonymous Subscription Schemes: A flexible construction for online services access," in Proc. Int. Conf. Security Cryptography, jul. 2010, pp. 1-12.

[9]. 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.

[10]. 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.

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

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

[13]. S. Golovashych, "The technology of identification and authentication of financial transactions from smart cards to NFC terminals," in Proc. IEEE intell. Data acquisition Adv. Comput. Syst., Sep. 2005, pp.407-412.

[14]. K. S. Kadambi, J.Li and A.H. Karp," Near-field communication based secure mobile payment service," in Proc. 11th Int. Conf. Electron. Commerce, 2009, pp.142-151.

[15]. 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.

[16]. www.computerhowtoguide.com/2016/07/bitcoins-advantages-disadvantages.html

[17]. https://link.springer.com/chapter/10.1007/3-540-62494-5_6

[18]. Ross Anderson, Harry Manifavas, and Chris Sutherland. A practical electronic cash system, 1995. Available from author: Ross. Andereson@cl.cam.ac.uk

[19]. D. Chaum, A. Fiat, and M. Naor, "Untraceable electronic cash," in CRYPTO, ser. Lecture Notes in Computer Science, vol. 403. Springer-Verlag, 1988, pp. 319–327.

[20]. Camenish, J., Maurer, U., and Stadler, M. (1997). Digital Payment Systems with Passive Anonymity-Revoking Trustees. Journal of Computer Security, 5(1):254–265.