FAKE ELECTRONIC DATA CAPTURE DEVICE FOR OFF-LINE E-COMMERCE

P.Jayaprakash[1], Prof.Dr.E.Ramaraj[2]
Department of Computer Applications, Alagappa University, Karaikudi, India
[1]jayaprakash878@gmail.com
Department of Computer Science, Alagappa University, Karaikudi, India
[2]eramaraj@rediffmail.com

Abstract - **Off-line micro-payment is used more often today than ever before. Capable hackers are clever to break the security on credit and debit cards and right to use enormous capacity of card records. Through the amplified awareness of cybercrime, the production has prepared strides in using further secure techniques for keeping data. This has equipped it harder for malefactor, but there are still many occasion for attacks. This new idea provides a two-element validation to the client. The association among a coin element and an identity element avoids theft coin elements. A particular coin element can be read only by an individual identity element. This methodology still affords unknown transactions as every identity element is hard to a system. Similarly the identity element and the coin element are constructed by physically uncloanable functions. Both of them take over the following features: Clone resiliency, Emulation resiliency, and Unpredictability.**

Keywords:Credit and Debit Cards, PoS System, Attackers, Customer, Vendor, FRoDO

I. INTRODUCTION

A mutual constraint of existing methods is that the payment Protocol each wants at minimum one of the elaborate Devices to be on- line or it demands each transaction to be associated to a bank account [3]. Credit cardrecords theft is one of the greatest primitive procedures of cybercrime. End Users browse the available materials and attain their needs with smallest energy compared to conventional selling devices [6]. Credit card information shoplifting is one of the greatest aboriginal customs of cybercrime. Cybercrime teams classify sophisticated actions to take huge capacity of data. Around are some roadways attackers can take to pinch this data. One possibility is to gain contact to a databank where card data is stockpiled. But additional option is to aim the knowledge at which a retailer first expansions that card information the POS system.

POS threat is nowa day's one of the tremendous of pinched payment cardssources for cybercriminals. Despite advances in card safety tools and the requirements of the Payment Cards, there are stagnant gaps in the safekeeping of POS systems. It consolidated for further common security Shortcomings.

The word "POS system" most generally argues to the in store device wherever clients pay suppliers for belongings and services. But a lot of POS relations are delivered out spending cash; many of these payments are made by trades robbing their cards over a card reader. These card readers might be separate system but modern POS systems, principally those in higher retailers, are among them systems which can grip a dissimilarity of buyer transactions such as gift cards, sales, and promotions. Most in essence from a protection standpoint, they can handle many payment categories.

II. RELATED WORKS

In authors "peipeishi, Bo zhu and AmrYouseef" presented a new method like pin access scheme which is robust against shoulder-surfing attacks. Even if the shoulder-suffer can record the whole PIN access function for one time with a video device. This method has two variants, both of which achieve a good stability between security and usability. Different variants of the proposed scheme display a trade off in resisting various types of adversaries, and thus selection of an appropriate variant could be optimized type and frequencies of risk encountered in the application. The new method seems like to be intuitive and easy to use. No need to require users to memorize any other information besides their original PIN'S [1].

In author "Von Solms" presented investigate the different POS devices used by business environment. In transaction receipts relevant evidence printed on the merchant receipt after a particular transaction. In that transaction receipts evidence contained which is save from POS terminal is sufficient to complete the successful online purchase at multiple online shopping sites. CVV number on the back of the credit card can be obtained while transaction is in progress. Even promote online sites can be efficiently used without the permission or acquaintance of the credit card holder. Nevertheless the information replicated on assured POS transaction receipts that can be used for limited duplicitous online purchase [2].

In authors “VanesaDazaand Roberto Di Pietro” presented a novel mobile micropayment method where totally involved parties can be entirely offline. This method improves over state- of- the art approach in terms of payment security and flexibility. In order to Force relies individually on limited data to perform the invited action. In work refer to force architecture, mechanisms and rules. Which has been achieved by leveraging PUF properties and special read once memory where our digital credits have been memorized using highly unpredictable layout. Enhanced version of the FORCE, which is allow the arithmetical credit to be spent in various off line transaction [3].

In authors “Ronald L. Rivest and Adi Shamir”defined about POS device. This technique was implemented through the two micropayment scheme, which have done by the number of public key and hash function operation. Unique efficiency is required to support the micropayment scheme otherwise the mechanism of the charge will exceed the value of payments. Micropayments schemes are light-weight process compared to full macro payment schemes. Decrease the over-all of public key procedures compulsory per payment. Over the hash functions procedure 100 times quicker than the RSA signature authentication and 10,000 times quicker than RSA signature generation [4].

In author “David Busuttil” presented the execution of a secure wireless point of sales device exhausting infra-red link between the mobile device and dongle connected to a POS, which in turn is connected via a network to the contract server. Transaction is agreed out through the server’s communication relation combined with the banking system. A basic result In view of a cryptography hash work will be embraced will secure every bundle starting with Eavesdropping.Newer short-range wireless technologies could be used to exchange the Infra-red bond easily and also guarantee a fast user discovery without the need of paring or user interaction [5].

III. FEDCMETHOD

A. Monitoring

Malware which is expressly manufactured to steal information from POS devices is widely offered in the secretive marketplace. More number of network-sniffing, spasms tools is hand-me-down to accumulate credit card records as they traversed internal unencrypted networks. Sometimes, the RAM-scraping malware is used to accrue credit information as they are read into PC memory. Every composed folder is then close by kept in a file until period for exfiltration. The data wants to be transmitted to several additional PCs, via interior network up to reaching the scheme that has access to outward systems.

Because the attacker was pointing a POS device and these spasms take period to collect data, they necessity their code keep on insistent on the conceded station. Not like database cracks where lots of records are instantly manageable, POS device breaches call for the attacker to postpone until transactions take place and then bring composed the records in concurrent at credit-card is used. For that object of these, rapid finding of the violence can extreme the intensifications of the destruction. The Malware persistence will be achieved with simple procedures to guarantee that the malicious method is continuously running and restarts whichever time the method restarts.

B. Encryption

There are some stages that POS machinists can takings to decrease the danger of attacks alongside POS systems. Occupation two-factor verification at entirely admittance points to the card holder data environs and for any persons with access truths to the CDE and employ two-factor authentication for all system arrangement modifications indoors the CDE setting.

When individual expenses by snatching a credit-card at a POS device, data restrained in the card’s magnetic stripe is read and then dispersed over a dissimilar systems and links before getting the seller’s payment processor. After this data is conveyed over a public network, the record need be privileged using network level encryption.

Many sellers shortly use network level encryption methods equal enclosed by their interior networks. When that alteration protected the data it went from one device to another, the card records are not encrypted in the systems and can unmoving be form in plain text inside the recollection of the POS device and another computer answerable for processing or transient on the data. This weakness has led to the advent of “RAM-scraping” infected and agrees invaders to extract this data from recollection whereas the data is being process privileged the mortal rather than when the data is itinerant over the network.

C. Architecture Diagram

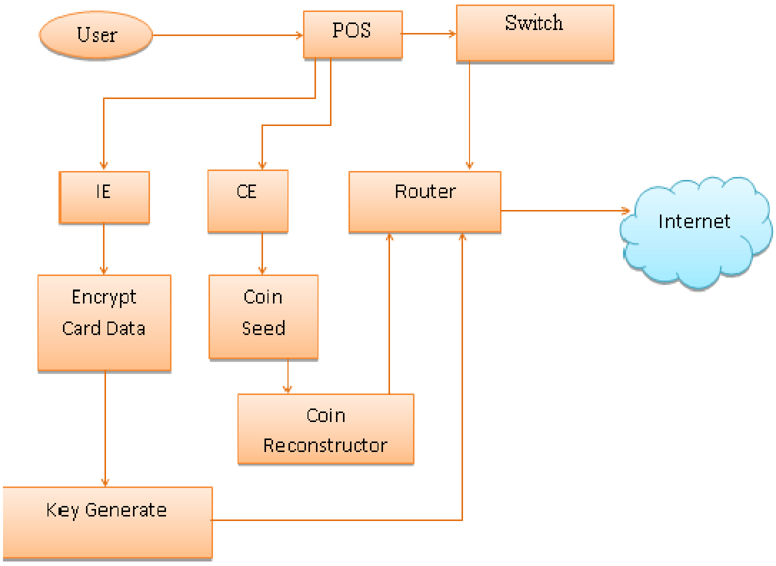

Fig.1. Architecture Diagram

IV. IMPLEMENTATION OF END TO END ENCRYPTION

The cryptographic keys used to encrypting and decrypting the messages stored on the end points, bogus made conceivable through the usage of public key encryption. Even though the key exchange in this situation is measured unbreakable expending identified algorithms and presently obtainable totaling power, here at least two possible weaknesses that exist external of the arithmetic. The every endpoint must achieve the public key of another endpoint, but a potential attacker who could afford one or both endpoints with the attacker's public key can applianceagent in the mediumintrusion. Also, all stakes are off if each endpoint has been negotiated such that the attacker can realize messages previously and later they have been encoded or decoded.

Generally employed technique for confirming a public key is in declaration the legitimate key created by the future heritor is to presentation the public key in an authorization that has persisted digitally signed by a well-recognized certificate authority. Since the CA's public key is commonly distributed and normally known, its reliability can be calculated on, and a certificate signed by that public key can be assumed authentic. Meanwhile the certificate companions the recipient's name and public key, the CA would apparently not sign a certificate that linked an altered public key with the matching name.

A. Algorithm For Encryption

INPUT: PT (Plain Text), K (key)

- Choose a key with length equal to plain text.
- Convert both Plain text and key into its ASCII values and then to their equivalent binary values.
- In preprocessing.

  PT_1 = PT_b (XOR) $_{(REV)}$ Kb //plain text is XOR-ed with the reversed key value.

  PT_b = binary value of plain text.

  K_b = reversed binary value of key.
- Calculate n :

  n = MAX (ASCII in K)/16 // n is calculated by dividing the highest ASCII value by 16.

  n = number of bits shifted right.
- Calculate N :N= $((r_b \bmod u)^a \bmod u)$

  (or) N= $((S)^a \bmod u)$

  N = Number of rounds to be performed.
- Shifted key values are XOR-ed with the result of previous round XOR-ed value.

  PT_2 = PT_1 (XOR) $_{(rev)}K_{(nRShift)}$ // at round 1.

  Where n = 1,
- $K_{nRShift}$ = n bits of key value are right shifted.

- At Nth Round, cipher text is obtained

  $CT_b = PT_N$ (XOR) $_{(rev)}K_{(nRShift)}$

  CT_b = binary values of the cipher text,

  $K_{(nRShift)}$= multiples of n bits values are right shifted.
- Convert the binary values of the cipher text to its corresponding decimal values, and then to its respective characters Eg: 0 = A, 1=B

  END

B. Algorithm For Decryption

INPUT: K (Key), CT (Cipher text)

- Cipher text is converted to its equivalent integer values, and then to its binary values.
- Calculate N:

  N= $((r^a \bmod u)^b \bmod u)$

  (or) N= $((Q)^b \bmod u)$.
- At round 1 in decryption

  $PT_N = CT_b$ (XOR) $_{(rev)}K_{(nRShift)}$.
- After Round N,

  PT_b = PT1 (XOR) $_{(rev)}$K.
- Obtained PT_b is converted to its equivalent ASCII values, from which the plain text PT is recovered.

END.

V. RESULT AND DISCUSSION

FEDC Method has provided the measurement of the PoS system. When the End – to – End Encryption algorithm is applied in the PoS system, it could take the less consumption for holding the card details of the card holder. Whereas FroDo System takes much more time to hold the data in existing method.

FEDC Method provides extreme security which has 1024 bit size of key.This method has 16 sizes ASCII value and coin element are generate randomly which could not be used again.Based on the experiential result security is provided high and without the knowledge of Authenticated person.

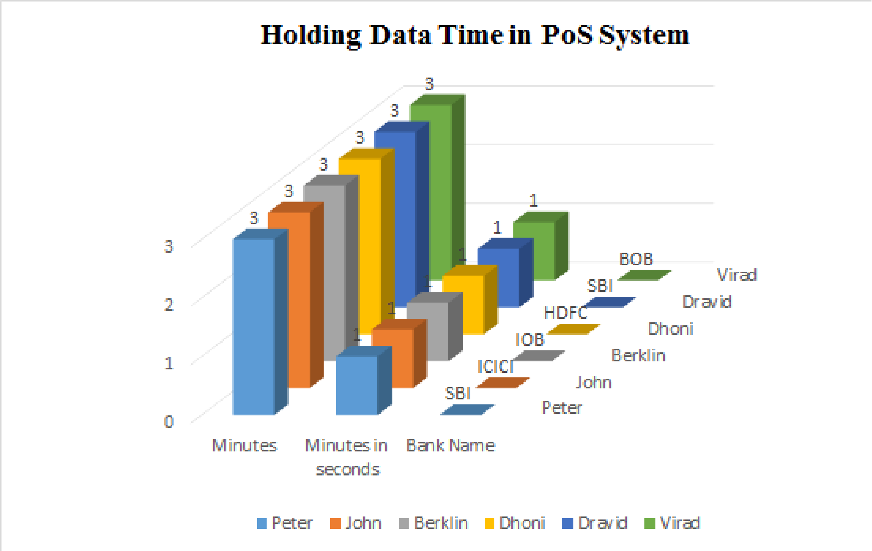

Fig.2. Holding Data Time in PoS System Diagram

POS system will contain the sensitive information of card holders after the transaction. To avoid this problem, data should be erased from device. Following features are introduced in device that provide the security to the card holder, like printing the data of particular transaction without stored information in database, which may help to steal the data by the vendor.

VI. CONCLUSION

FRoDO is the latest of offline-payment. FRoDO is the first information-breach-resilient that fully network disconnected micro payment method. This has been extended by a novel erasable PUF design and a novel rules plan. The FEDC analysis shows, that FEDC is the best proposal to more secure transaction solution, also introducing springiness when allowing for payment medium (types of digital coins). Finally, specific open issues have been recognized for future work. The chance is to allow digital modification over many off-line transactions while keeping the alike level of security and usability.

REFERENCES

[1] Shi, Peipei, Bo Zhu, and Amr Youssef. "A rotary PIN entry scheme resilient to shoulder-surfing." ICITST 2009. International Conference for. IEEE, 2009.

[2] Von Solms, Suné. "An investigation into credit card information disclosure through Point of Sale purchases." ISSA, 2015. IEEE, 2015.

[3] Daza, Vanesa, et al. "Force: fully off-line secure credits for mobile micro payments." SECRYPT, 2014 11th International Conference on. IEEE, 2014.

[4] Rivest, Ronald, and Adi Shamir. "PayWord and MicroMint: Two simple micropayment schemes." Security protocols. Springer Berlin/Heidelberg, 1997.

[5] Debono, Carl J., and David Busuttil. "A secure wireless point of sale system." EUROCON, 2011 IEEE. IEEE, 2011.

[6] Umamaheswari, M., S. Sivasubramanian, and B. Harish Kumar. "Online Credit Card Transaction Using Finger Print Recognition." IJET 2.5 (2010): 320-322.

BIBLIOGRAPHY

Jayaprakash P received the Master's Degree in Computer Applications from the Alagappachettiar College of Engineering And Technology, Karaikudi, Tamilnadu, India, in 2016, and currently pursuing the M.Phil. degree at Alagappa University, Karaikudi, Tamilnadu, India. Who has Research interest in Network Security.

Dr.E.Ramaraj, He is professor and head of the department in computer science at AlagappaUniversity, Karaikudi,Tamilnadu, India. He has published morethan 138 articles in both national and international conferenceand who has 30 years of experience in teaching. His research interest isData Mining, Network Security and Big Data & Analytics. He has published more then 138 articals in both national and internation conference.